Future security challenges: Are you ready?

Michele Colajanni

Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi (CRIS)

Università di Modena e Reggio Emilia, Italy

SDCI 2012, Cortina, 17th January 2012

Motivation

- "Software architects must have a strategic vision (i.e., to look forward ten years from now)" [Russo-Wright]
- Can academic researchers be less visionary?

- Our goals:
  - Possible directions for security research in a changing horizon
  - Separate Reality from Miths and Hypes
  - Separate Research from Business issues

Outline

- Review of attacks (*by contract*)
- Scenario 1: “Exponential”
- Scenario 2: “P+I”
- Scenario 3: “Ubiquity”
- A solution that fits all (?)
- Final remarks

ATTACKS

Hackers were once a nuisance

Source: *Time Magazine,* December 12, 1994

Newsday technology writer and hacker critic found

- email box jammed with thousands of messages
- phone reprogrammed to an out-of-state number where callers heard an obscenity-loaded recorded message

Then it got more serious

Source: PBS website report on Phonemasters (1994–1995)

An international group attacked major companies: MCI WorldCom, Sprint, AT&T, and Equifax credit reporters

- got phone numbers of celebrities (e.g., Madonna)
- gained access to FBI's national crime database
- obtained information on phones tapped by FBI and DEA
- created phone numbers for their own use

... and profitable

Source: PBS website report on Vladimir Levin, 1994

Russian hacker accessed Citibank computers and transferred $10M to his accounts using passwords and codes stolen from Citibank customers

- Citibank and FBI tracked Levin
- all but $400,000 recovered

Software was blamed for problems

Source: *Business Week* cover story, December 6, 1999

"Glitches cost billions of dollars and jeopardize human lives. How can we kill the bugs?"

DDoS attacks become a reality

Source: *Seattle Post-Intelligencer Staff and News Services,* February 9, 2000

Operations of major e-commerce and websites seriously disrupted

Examples:

Links are made with organized crime

Source: *Ecommerce Times*, March 9, 2001

FBI advises that Eastern European hacker groups stole information from e-commerce and online banking sites

- 40 firms in 20 states, lost over 1M credit card numbers
- credit card information sold to organized crime entities
- the criminal groups usually try to sell security services to victim sites

The relationships grow

Source: *New York Times News Service,* May 13, 2002

Eastern European Internet sites traffic in tens of thousands of stolen credit-card numbers weekly

- financial losses claimed of over $1B/year
- cards prices at $.40 to $5.00/card – bulk rates for lots of hundreds or thousands
- organized crime groups buy from black-hat hackers

…with links to terrorist activities

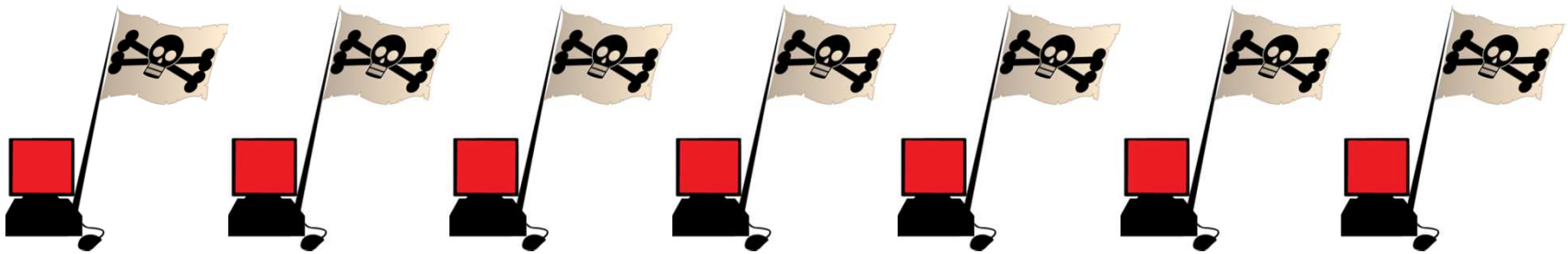
Source: Testimony of Mr. Dennis Lormel, FBI; Senate Subcommittee on Technology, Terrorism and Government Information, July 9, 2002

- Terrorists use identity theft & social security number fraud to
  - obtain employment & access to secure locations
  - get driver's licenses and bank and credit card accounts to facilitate terrorism financing
- Terrorist cell in Spain used stolen credit cards in fictitious sales scams and for many other purchases for the cell

Botnets and Botnet+ for hire

Source: *Technology Review,* September 24, 2004

- Pirated computers rented for $100/hour, average rate in underground markets
- Used for sending SPAM, launching DDoS attacks, distributing pornography, etc.



“Phishing” and Identity theft

Phishing: fraudulent email and websites used to lure recipients into divulging sensitive information such as credit card numbers, social security numbers, bank account numbers and PINs

A rapidly growing problem

Anti Phishing Working Group (www.antiphishing.org)

400% increase	over holidays	(Dec. 03 report)
50% increase	in Jan. 04	(Feb. 04 report)
60% increase	in Feb.04	(March 04 report)
43% increase	in March 04	(April 04 report)
180% increase	in April 04	(May 04 report)

300% increase May 04 to Jan 05

- etc, etc, etc

Mobsters gain control

Source: *eweek.com,* April 13, 2006

"Cybercrime more widespread, skillful, dangerous than Ever"

- Russian mafia and Web gangs take control of billion dollar crime network powered by hackers
- Underground markets trade in "private exploits" that evade anti-virus software, botnets at $25/10,000 hijacked PCs, zero day exploits, DoS attacks
- Recruiting "mules" to move and launder funds

Espionage is on the rise

Source: *Business Week* Cover Story, April 10, 2008

"The New E-spionage Threat"

- Unprecedented rash of attacks against U.S. Government and defense contractors
- Personalized email (**APT**) indicates prior intelligence work
- Air Force Cyber Command reports attacks against military systems up 55% over prior year
- President Bush signs Cyber-Initiative order on January 8
- McConnell testifies to Senate that threats come from China

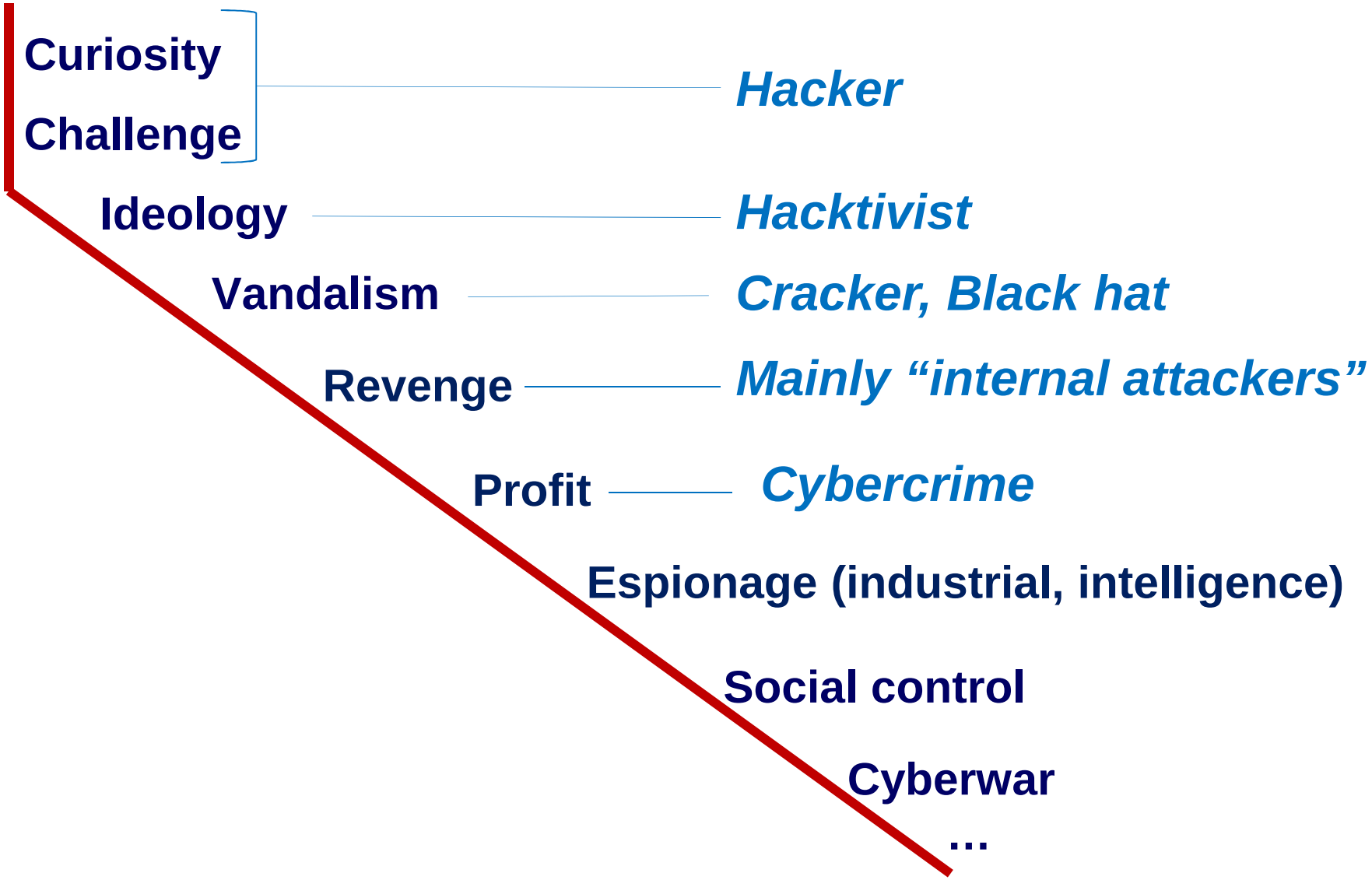
Some evolution of attacks

- **Hardware trojans**
  - "15 criminal cases involving counterfeit products (Cisco routers) bought by military agencies, contractors, and power utilities" [*New York Times,* May 9, 2008]
- Combination of human and technological attacks
  - From phishing to **spear phishing** targeting the "fat cats"
- Combination of multiple technological attacks
  - **Advanced Persistent Threat** (APT)

Threats – more of same plus new

- “Attacks for profit” – dramatic increase
- Computer/network facilitated crime – continued increases
- Connections between organized crime and technical mercenaries - increase
- Embedded malicious code – more instances
- Shift of attack patterns from OS and protocols to applications and new devices
- Stealthy, automated attacks aimed at individual companies/industries

Attackers and Motivations



2011: “The year of cyberattack”

“It doesn't matter if a business is in financial services, retail, education, gaming, social, government, telecom, media or travel. Daily headlines tell the stories of millions of lost credit-card numbers, millions of personal information records exposed, and gigabytes worth of intellectual property stolen.”

- Sony, Sega, Nintendo
- Zynga
- Citigroup, Sony, PBS
- AT&T
- CIA, US Senate, NASA, Nasdaq, NYSE
- RSA
- Stratfor Global Intelligence

CYBERATTACKS TIMELINE

MAJOR COMPANIES/AGENCIES RECENTLY TARGETED *(Date of attacks only indicate when they were first discovered or publicised)*

2010 Dec — Hacker group claiming attack
Mastercard.com, Paypal, Visa.com, PostFinance
Anonymous launches orchestrated attacks in support of Wikileaks founder Julian Assange

2011 Mar. — (unidentified)
RSA
Hackers steal data related to RSA secure tokens

20 Apr or earlier
Sony Playstation Network
Hackers steal personal information from millions of users in first of a series of attacks on Sony

22 Apr*
Fox Networks
Lulzsec stole personal information of 70,000 X Factor contestants, database and passwords from employees

May
Citigroup Inc.
Hackers take 200,000 customers' data

21 May
Lockheed Martin
Hacked but managed to stop attack before any critical data was stolen

30 May
PBS.org *Lulzsec defaced its website, posted a fake article and stole its database*

1 Jun
Google *Email system hacked, attack suspected to originate from China*

2 Jun
Sonybmg.nl, Sonybmg.be
3 Jun
Nintendo.com
Infragard-Atlanta (FBI)

10 Jun
Turkish government websites
Anonymous takes down several government sites in protest to Internet censorhip

11 Jun
International Monetary Fund
Hack suspected to originate from a "foreign government"

Spanish National Police
Anonymous hacks website in response to arrests of alleged group members

13 Jun
Bethesda Game Studio
U.S. Senate *(www.senate.gov)*
Lulzsec hacked and released internal data from its servers

15 Jun
Malaysian government websites
Hacked after an attack warning from Anonymous in response for censoring Wikileaks

Central Intelligence Agency
Lulzsec hacked the CIA's public website, www.cia.gov, making it temporarily inaccessible

19 Jun
SEGA
Hackers compromise accounts of some 1.3 million customers

3 Jul
Apple
Anonymous hacks into one of Apple's servers, publishes internal usernames and passwords

21 Jul
NATO
Anonymous and Lulzsec hack NATO servers, obtain 1GB of restricted data

HACKER GROUPS ASSOCIATED IN RECENT ATTACKS

Insignias

► Anonymous
Describes themselves as an online community who promotes internet freedom and freedom of speech. Participated in international hacktivism and protests since 2008

Insignia

► Lulzsec
Believed to be a splinter group of Anonymous, they often post taunting or mocking messages to corporations and agencies they have compromised

Source: Lulz Security, Anonews.org, news reports **Actual date*

REUTERS

ATTACKS: END OF THE GAME

A *vs*. V

- Single *vs*. Single
- Single *vs.* Group
- Group *vs*. Single
- Group *vs*. Group

Motivations

- Challenge
- Fun, Stupidity
- Demonstration, Publicity
- Opportunity
- Vandalism, Violence
- Ideology
- Revenge
- Profit
- Espionage
- Intelligence
- Control

End of the game

End of the talk?

Let’s go skiing

NO!

The scenario is continuously changing = *new targets for the attackers*

1. **Emerging socio-technical ecosystem**
   - Globalization and ubiquitous Internet-based services are changing the way of interactions among government, business, citizen
   - As security in advanced companies improves, ***weaker links*** in contractor-supply chains will emerge
2. **Physical infrastructures "enriched" with ICT**
   - Critical infrastructures
   - Industrial plants
   - Industrial products (e.g., "Cars: The new victims of cyberattacks", Jan. 2012)
3. **Ubiquity**
   - Mobile devices - Internet of things - Smart dust

CHANGING SCENARIO 1

"The exponential epoch"

Changes happen
(and in our world they happen always)

"The target is moving and is changing" [AB]

We are living in an *exponential* world, not *linear* anymore


IN 60 SECONDS...
1 NEW DEFINITION IS ADDED ON urban
1,600+ READS ON Scribd.
13,000+ HOURS MUSIC STREAMING ON PANDORA
12,000+ NEW ADS POSTED ON craigslist
370,000+ MINUTES VOICE CALLS ON skype
98,000+ TWEETS
20,000+ NEW POSTS ON tumblr.
THE LARGEST SOCIAL READING PUBLISHING COMPANY!!
320+ NEW twitter ACCOUNTS
13,000+ iPhone APPLICATIONS DOWNLOADED
100+ NEW LinkedIn ACCOUNTS
1 associatedcontent NEW ARTICLE IS PUBLISHED
THE WORLD'S LARGEST COMMUNITY CREATED CONTENT!!
QUESTIONS ASKED ON THE INTERNET...
100+ Answers.com
40+ YAHOO! ANSWERS
6,600+ NEW PICTURES ARE UPLOADED ON flickr
600+ NEW VIDEOS
50+ WordPress DOWNLOADS
25+ HOURS TOTAL DURATION
70+ DOMAINS REGISTERED
695,000+ facebook STATUS UPDATES
125+ PLUGIN DOWNLOADS
60+ NEW BLOGS
168 MILLION EMAILS ARE SENT
694,445 SEARCH QUERIES
1,700+ Firefox DOWNLOADS
1,500+ BLOG POSTS
79,364 WALL POSTS
510,040 COMMENTS
Google
Google Search
GO-Globe.com

User Generated Content

- **2000-2005**
  - “Official” contents: 95-90%
  - User generated content: 5-10%
- **2006**
  - “Official” contents: 68%
  - User generated content: 32%
- **2010**
  - “Official” contents: 20%
  - User generated content: 80%

You Tube: Some numbers

- There is more video content in YouTube than that produced in the entire history of “cinema”
  - **2007**: 6 hours of video uploaded every minute
  - **2008**: 10 hours of video per minute
  - **2009**: 16 hours of video per minute (like a Hollywood movie industry producing 86.000 films per week)
  - **2010**: 24 hours of video per minute
  - **2011**: **35 hours of video uploaded every minute**

    2+ billion videos viewed daily

Today

- 1,5+ Billion smartphones
- 2+ billion Internet users (1/3 world's population)
- Facebook: 700+ million users
- Twitter:
  - 200+ million of accounts
  - 100+ million tweets per day
- Zynga: 250+ million of users
- CityVille: 100+ million downloads in 43 days
- Saleforces: 90,000+ customers
- iTunes:
  - 350,000 apps
  - 10+ billion downloads

2020 (*probably before*)

ULTRASCALABLE. EXASCALE

Billions of Users

consuming

Tens of Millions of Services

delivered by

Millions of Service Providers

built on

Hundreds of Millions of Servers

containing

Exabytes of Data

connected by

Terabytes Networks

The main question

Are you ready?

(that is, is your approach to security research adequate to this kind of journey?)

You can get off now

DEFENSES

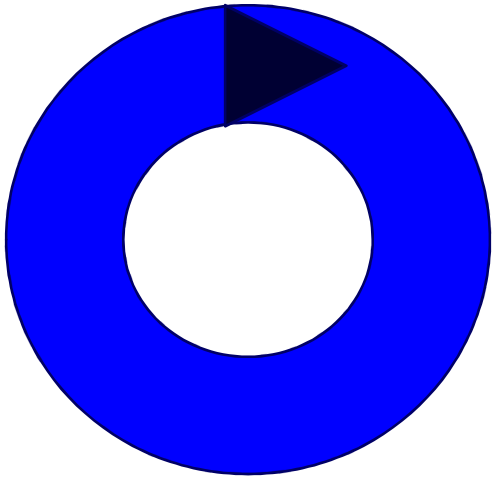
Security solutions

- Anti-malware
- Firewalls
- Content filtering for email and web
- Intrusion Detection/Prevention Systems (IDS/IPS)
- Virtual Private Network (VPN)
- Patch management
- Cryptography

But don’t forget that:
Security is a process, not a product

Not just a process, a *continuous process*

- Good planning ←→ Good management
- Risk analysis
- Risk management
- Security policies
- Security solutions
  - Previous ones +
  - Minimize exposure
  - Increase human awareness
- Assessment (internal and external)
- Containement: early detection, Incident Response Team



Security products and services

Key question: How will today's security solutions evolve, scale to meet new challenges?

- Increased dissatisfaction with effectiveness of perimeter security
- Growing dissatisfaction with intrusion detection systems
- Growing dissatisfaction with anti-malware products
- Greater emphasis on maintaining the integrity of known "goods" rather than trying to screen for known "bads" and praying for no unknown "bads"

System and product vulnerability

- Continued growth in vulnerability caused by increased size and complexity
- Firmware vulnerabilities is becoming a problem
- **Current response and recovery practices will not scale**
- New personal devices will abound
  - All will be Internet-connected
  - Some will run serious operating systems with significant memory and disk size

Better understanding

Data sharing is time consuming and expensive leading to islands of information and little shared understanding

Research projects to

- develop open standards for capturing, storing, and transmitting huge amount of heterogenous security information and analysis results
- form sharing and analysis coalitions to improve understanding and disseminate knowledge
- establish global indications and warning systems with predictive capabilities
- define requirements for automated support for recognition, response, reconstitution, and recovery

Better softwareproduction

Low-quality software continues to be as the root cause of most vulnerabilities, threats and incidents

Research projects to:

- demonstrate business case for improved software engineering process (higher quality)
- increase effectiveness of static and dynamic analysis tools
- achieve higher levels of application security

Better system architectures

Some problems are rooted in system architecture and design (when you put components together)

Research projects to:

- achieve **"X" by design** through more interactions among researchers and security practitioners, where **"X"** stands for:
  - Dependability
  - Scalability
  - Safety
  - Security
  - Privacy
  - …

Better systems management

Response team experience shows that some organizations are on the edge of security and others are clueless

Need activities to develop and promote security management practices that are

- supportive of an organization's mission & goals
- focused on risk reduction rather than on mere compliance
- measured, reviewed, and updated regularly

NOTE: These activities are not academic research

Better people

Management practice dictates the “what”, but the skills and abilities of the staff determine the “how well”

Need activities to

- support and promote the development of performance and training standards (such as DoD 8530 and 8570) as well as more security topics in degree programs
- encourage managers to invest in the training and skill building needed to stay on top of a constantly changing problem

NOTE: These activities are not academic research

Complex, ultra-large-scale systems

Large scale systems must continuously deliver results while suffering attacks, accidents, and failures

- **New design and implementation must merge with updates and configuration changes**

+ **Some individual components are becoming more secure (e.g., hardened operating systems, embedded systems, network components)**

+ **More hardware will help solve problems: biometrics, encrypting disks, etc.**

CHANGING SCENARIO 2

"The physical world enriched with ICT"

2000 decade: We are working to integrate the *p*-world with the *i*-world

2010 decade: Done!

Critical infrastructure

Not well defined borders

- Transportation
- Energy production and distribution
- Gas and oil storage
- Industrial plants
- Internet
- Communications
- Emergency services
- Finance, banking
- Waterways, dams
- Water supply
- Governement services
- Law enforcement
- …

Industrial Control Systems (ICS)

Def. ***(ICS):*** **command and control networks and systems designed to support industrial processes**

- ICS are responsible for monitoring and controlling a variety of processes and operations such as gas and electricity distribution, water treatment, oil refining or railway transportation
- The largest subgroup of ICS is **SCADA** (Supervisory Control and Data Acquisition) systems

Industrial Control Systems (ICS)

In the last few years, ICS have passed through a *significant transformation*

From proprietary, isolated systems to open architectures and standard technologies

From separated environments to systems interconnected with other corporate networks and, sometimes, with the Internet

Motivations:

- cost reductions
- ease of use and management
- enabled the remote control and monitoring from various locations

Hypes and Hyperboles

- "ease of hacking SCADA systems"
- "foreign attackers are already in the Grid"
- "critical infrastractures: state of near chaos"
- "utilities investing in compliance minimums"
- "attackers having free rein"
- …

Just to push the "fear" button harder

(*Thanks to some intelligence agency that created Stuxnet*!)

A researcher must distinguish *hype* from *reality*

- When considering risk prioritization, the largest risks to the overall safety and reliability of the electrical grid are threefold:
  - **Natural**: environmental, weather, vegetation, human
  - **Mechanical**: equipment age and equipment failure
  - **Electrical**: transmission capacity, load management

- **Those risks are, in general, not from cyber-based attacks**

Reality

- In the energy industry, everything is measured against ***impact to reliability***, and there are different ways the industry measures it, e.g.,
  - **SAIDI**, **SAIFI**, **CAIDI**, **MAIFI**, …
  - Everything related to improving reliability revolves around improving those metrics
- To date, cybersecurity issues have had no impact on those metrics (at least in North America): 99.995% availability
- This is not to deny that there have been cybersecurity events within the industry, because there have been quite a few, but none have ever impacted the reliability metrics

Reality

- Most utilities are required to comply with the **NERC Critical Infrastructure Protection** (**CIP**) standard
- The CIP standards are created by the member utilities, approved through a standards voting process, and then “ratified” by DOE
- Utilities are audited to these standards, and can be fined for non-compliance, with fines ranging up to a million dollars per day for critical violations
- Hence, Utilities work very hard to meet these standards, even thanks to strong financial incentives to do so

Expectation

- “High Impact, Low Frequency Event Risk to the North American Bulk Power System” (June 2010) identified three events:
  - Pandemic, geomagnetic disturbance
  - Electromagnetic pulses
  - **Coordinated attack**: “a concerted, well-planned cyber, physical, or blended attack conducted by an active adversary against multiple points on the system.”
- **No such attack has ever been experienced**
- **This kind of event would be an act of war**, and no private utility is able to, or could be expected to, defend against an attack funded by a nation-state (the cost of such defenses could easily double the cost of electricity)

In conclusion

- The security of energy, water, health care, telecommunications, transportation, finance systems is essential to modern living
- But things aren’t nearly as bad as media loves to report
- They must pay careful attention to the cybersecurity of their systems, but this is true of any industry

Critical infrastructures as *special customers*

- Business view: "Just new customers that need to apply well known technologies"

- Research view: "The combination of P+I worlds open some interesting issues", e.g.,
  - **Complexity and heterogeneity**
  - **New protocols and new types of data require new models**
  - **Impossibility to outsource all their services**

CHANGING SCENARIO 3

"Ubiquitous services"

2015

- 2+ billion Internet users (1/3 population) → 1/2 population by 2015
- Global mobile data traffic will increase 26-fold
- Nearly one mobile device per capita in the planet
- Mobile network connection maximum speeds will increase 10-fold
- Mobile-to-mobile traffic will reach 10 petabytes per day
- Two-thirds of the world’s mobile data traffic will be video

A trend that cannot work

- We want to access anytime, anywhere, anydevice to our data and services
- **Present scenario**
  - **60% of company data are on PC, laptop, iPad, smartphone, with increasing percentage of mobile devices with respect to PCs**
  - **10% of mobile devices are lost within 12 months**
  - **60% of pen-drives contains company data**
  - **66% of pen-drives is lost forever**
- **The laptop/smartphone/USBdrive model simply does not work!**

Different problems and different solutions

- Companies that do not need to (or cannot) allow *anytime-anywhere-anydevice* accesses
- Companies that need to allow *anytime-anywhere-anydevice* accesses to few employees
- Companies that need to allow *anytime-anywhere-anydevice* accesses to every employee

ONE SOLUTION THAT FITS ALL (?)

2020 technologies
(Hypothesis: no *disruptive* technology in the meanwhile)

- **NETWORK**
  - Mobility → Ubiquity
  - IPv6
- **COMPUTER**
  - Tens of billions of interconnected heterogeneous devices: from tiny *smart dust* devices to huge servers
- **CLIENT**
  - Browser-like technology (different interfaces)
- **SERVER**
  - Cloud-like technology as a server

Server side: data centers

Client side (?)

- Display 12,1 pollici
- 1,48 kg
- Oltre 8.5 ore di utilizzo
- CPU Dual-Core Intel® Atom™
- Wi-Fi dual-band + 3G World-mode
- Webcam
- Due porte USB 2.0
- Porta Mini-VGA
- Tastiera Google Chrome
- Trackpad di grandi dimensioni
- Sistema operativo Chrome OS
- 8 secondi per l'avvio
- "Defense in depth"

It pretends to be a normal laptop, but …

Security solutions

- Defense in-depth (user, technology, operations)
- Walled garden: *Google* "sandbox" and scanning for any visited page
- Cyphered file system (for few resident data)
- Storage cloud for any data
- Process cloud for any application
- Recovery button

CLAIM no. 1

- **In the future "every (interesting) IT application will be a critical infrastructure"**

- Russo's attributes
  - Large-scale
  - Software intensive
  - Dependable (safety, business mission critical)
  - Long-lived systems
  - Quality attributes cannot be achieved in isolation

CLAIM no. 2

- **In the future "every (interesting) IT application will be characterized trust and reputation"**

- **Untrusted services will tend to disappear**

2020 *hope*

Academy has to help computer industry to become a mature industry

The consequence of complexity

- **The present trend cannot persist**
  - Security sellers will be unable to explain what they will sell
  - Security buyers will be unable to understand what they will buy
  - Security problems left to *un-technological* users
  - Fake interpretation of compliance: "we don't know what we are doing, but THEY know, so please don't complain with us"

- **Complexity must be masked** (in some sense, this is true or will be true for most computer-related products)

2020 Security

It will not be anymore a problem of the user

(At least, not from the point of view of technology: human-related attacks -*social egineering*- will remain)

- **Security prevention**, e.g.,
  - Apple model
  - Trusted computing
- **Security embedded in provider's services**

Computer product and Security

- Nobody wants to buy security because it is *fear-based*
- Security is a byproduct of the computer industry, that is *greed-based*

- Separation between product and security is a demonstration that the computer industry is still **immature** (probably, because we move too fast)

Mature industry

- Can you imagine a scenario similar to what happens in computers in another industry?
- *Car dealer*: “Hey, before arriving at home, remember to buy brakes for your new car ... ”

- **Security is embedded**:
  - We expect breaks in the cars, a house with the door, a door with its lock, a safe electric tool, a gun that does not explode, potable water from the tube
  - and we sue companies that do not satisfy our expectations

Driving forces of the future trends

1. **Users – *how they are***
2. **Users – *what they expect***
3. **Services**
4. **Costs**

1. Users – *how they are*

- User are becoming much more sophisticated in the last twenty years but not in the sense we expected
- Not technically sophisticated, but communication and socially sophisticated

- Huge change with respect to the past:

➔*Early adopters* were technological-aware

➔*Modern adopters* do not want to know technical details. **They want *providers* to take care of all boring details**

2. Users – *what they expect*

- Modern users are platform free:
  - They do not know what operating system Google (or Facebook or Skype) use
  - They do not know where their data centers are
  - They do not know where their data are and what providers do with their data
  - ***And they don't care***

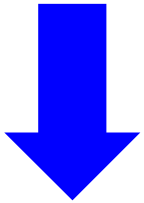
  - 99.9998% of users care only about services and quality of services: basically, ***availability*** and ***response time***
  - 0.0002% of users (≈700K) must care of everything (including security and scalability)

The quality of service is important

- Today, any company and organization (even those not related to the computer industry) is evaluated on the basis of the quality, availability and usability of the services provided through the Web
- Providers that want to live in a competitive market must guarantee their users a **high quality experience**
- It is considered unacceptable:
  - unavailable service
  - slow service
  - unsecure service

3. Services

- Computers are tools, commodities, like a desk or a staple. This is because ROI cannot work:
  - A desk is a desk. A car is a car. You need it or you do not need it. The same is for computers
- If the users want a “staple” that works and work well to access to the services they care of, then the services must work always, 24/7, and be fast for any amount of users



Provided services must <u>come with</u> dependability, scalable performance, *and security*

4. Costs

- From a company perspective, personal devices are so cheap that they are effectively free
- Same for network costs
- **This is the end of the game**, because it cannot become cheaper than free

- The high costs (*hardware*, *software*, *humanware*) are in the **server infrastructure**. So it makes a lot of sense to consolidate them in some cheap place that is managed 24/7 by competent people

You cannot stop this trend **(not *if* but *when*)**

The present alternative

OVERPROVISIONING

– Data centers with 10^3-10^4 servers are everywhere. There are also data centers with 10^5-10^6 servers

UNDER-UTILIZATION

– Servers (utilization<20% is the norm)

– Network components in data centers (utilization<10%)

Put it all together, and you get ...

Cloud computing (*essential definition*)

- **Your data are stored in someone else disk**
- **Your applications run in someone else server**

Main attributes for the Cloud

- **IT capabilities**: provided as a service
- **Elastic/Adaptive/On-demand**: as any other utility
- **Cloud**: server location is transparent for the user

Visionaries

- “Computing may someday be organized as a public utility”

  [John McCarthy, MIT Centennial, 1961]

- **Users will “trust” service providers with their data like they learned to trust banks with their money**

Deployment models

Examples

Business Process as a Service **(BPaaS)**

Software as a Service **(SaaS)**

Platform as a Service **(PaaS)**

Infrastructure as a Service **(IaaS)**

Not only technology

Cloud computing, as the Web,

is much more than

a technological innovation

Software engineering models

- **Cloud computing intrinsically promotes:**
  - a *process-oriented* model for software analysis
  - a *service-oriented* for software development (*Service Oriented Architecture* model + various toolkits/libraries/components offered by cloud providers)

Future

- Like for any mature industry, dependability, performance, scalability, security will become part of the service:
  - **Availability by design**
  - **Security by design**
  - **Performance by design**
  - **Privacy by design**
- Security will not disappear, but it will be managed by the providers and not anymore by the customers (users and companies)
- Amazon, Apple, and Google will do it for your services and data as Mercedes and Ferrari guarantee for your cars

Caveat

- To look at the providers and not to the customers do not mean that there is no space for work with the customers
- **Just, it’s not research**

- We can solve 96% of the problems with existing security products, methodologies, best practice, standards [NSA specialist, 2009]
- *It’s not our fault, it’s not our business if customers do not use them or do not use well …*

Motivators

- A provider sells on the basis of
  - **Price**
  - **Trust**

Different types of services

- ***Commodity services*** (e.g., water, heat, electricity, cleaning): the main motivator is **price**
- ***Middle services*** (e,g., phone call costs, credit cards, rental cars, banks): the main effort is to hide the real price
- ***Premium services*** (e.g., legal, medical, tax consultant, security): **trust** is much more important than price

Trust and Reputation

- Hopefully, IT will become a **trust&reputation market** with some interesting characteristics:
  - The customers has not the expertise to evaluate the service, hence they have to rely on **reputation signals**
  - **IT uses a lot of signal for trust and reputation:**
    - trusted blog or magazine (trust comes when there is a clear separation of opinions from advertisements)
    - recommendation from a friend or a people they trust
    - general reputation of a brand
    - certification
    - academic people more than company consultant
    - …

Example 1: PCI standard

- The credit card is the currency of the Internet: if you want to buy something, you need a credit card

- The credit card companies were scared that people did not use the credit card on the Internet

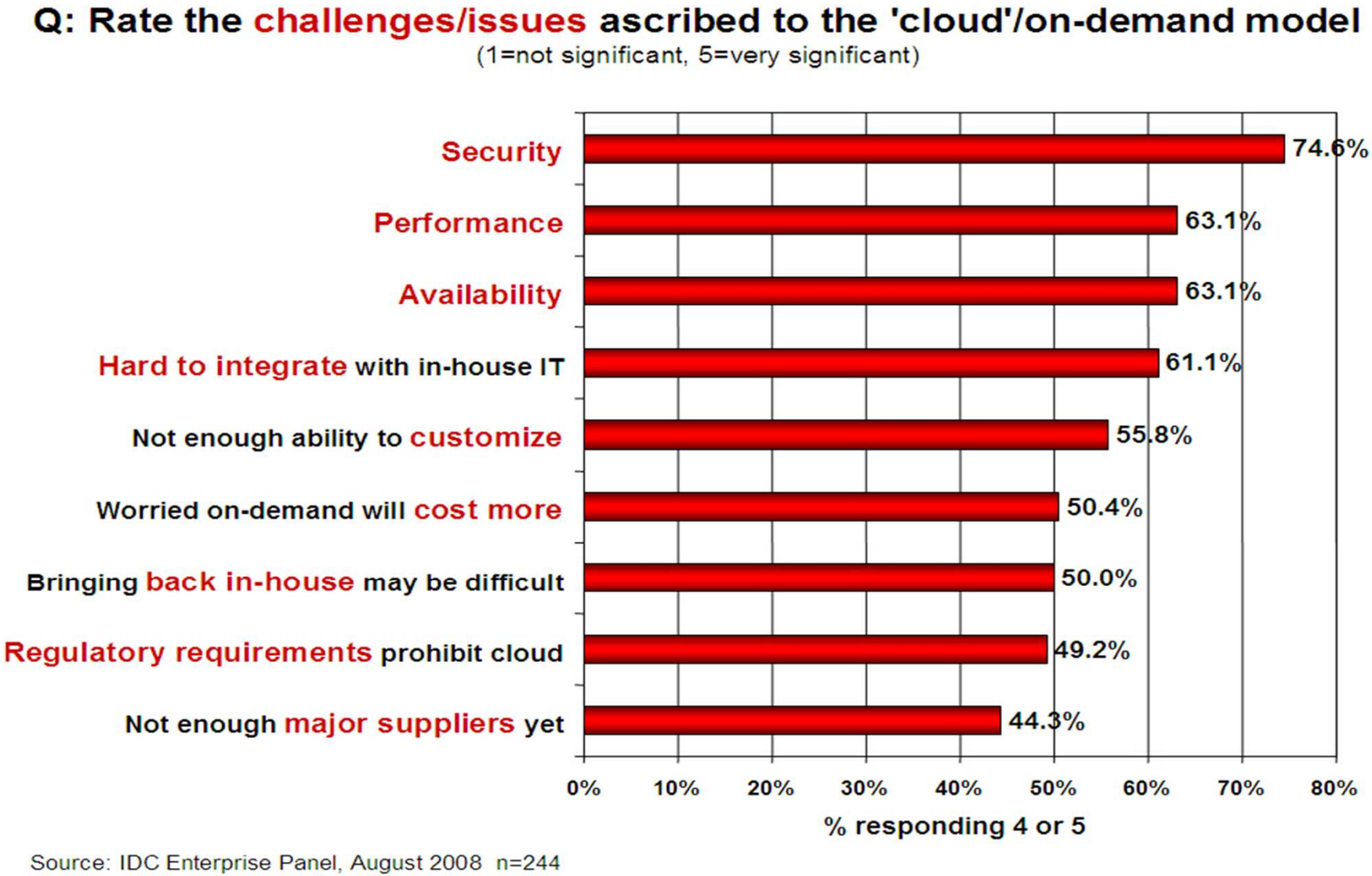
➔They invented the **Payment Card Industry** (PCI) as a **self-regulatory** standard

- The reputation of VISA was more important than the reputation of the merchants

Example 2: Disk laptop encryption

- People do not encrypt their laptop disks even if it a usable function today
- Consultants from PWH and E&J began to encrypt their laptops ten years ago
- This makes sense
  - If a customer loses his laptop, loses his data
  - If an important consultant loses his laptop, loses his data, the data of his customers, and likely many customers
- It is a matter of reputation

Main challenges for cloud



Security in the cloud

It is both the #1 goal *and* the #1 concern for IT

- **Most (87%) believe cloud will not impact or will actually *improve* their security posture**
- **Yet, they rate security as their #1 concern.** Top threats:
  1. Mass malware outbreak at your cloud provider
  2. Hacker-based data theft from your cloud provider
  3. Sharing sensitive data insecurely via the cloud
  4. Rogue use of cloud leading to a data breach
  5. Data spillage in a multi-hosted environment

[*State of the Cloud Survey*, Symantec report, 2011]

Cloud issues

- Some key issues:
  - trust, multi-tenancy, encryption, compliance
- Clouds are massively **complex systems** that can be reduced to **simple primitives** that are replicated thousands of times and **common functional units**
- Cloud security is a tractable problem
  - There are both advantages and challenges

Advantages

- Shifting public data to an external cloud reduces the exposure of the internal sensitive data
- It solves the anytime-anywhere-anydevice problem
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Redundancy and Disaster Recovery are emebedded in the system

Challenges

- Proprietary implementations cannot be examined
- Loss of physical control
- Trusting vendor's security model, but everything is a matter of trust:
  - Do you trust in all producers of the software installed on your PC?
- Customer inability to respond to auditing
- Obtaining support for forensics and investigations
- Indirect administrator accountability

More psycological issues

Security-relevant Cloud components

1. Cloud provisioning services
2. Cloud data storage services
3. Cloud processing infrastructure
4. Cloud support services
5. Cloud network and perimeter security

6. Elastic elements: storage, processing, virtual networks

1. Provisioning services

- **Advantages**
  - Rapid reconstitution of services
  - Enables availability
    - Provision in multiple data centers / multiple instances
  - Advanced honeynet capabilities

- **Challenges**
  - Impact of compromising the provisioning service

2. Data storage services

- **Advantages**
  - Data fragmentation and dispersal
  - Automated replication
  - Provision of data zones (e.g., by country)
  - Encryption at rest and in transit
  - Automated data retention
- **Challenges**
  - Isolation management / data multi-tenancy
  - Storage controller
    - Single point of failure / compromise?
  - Exposure of data to foreign governments

3. Cloud processing infrastructure

- **Advantages**
  - Ability to secure masters and push out secure images
- **Challenges**
  - Application multi-tenancy
  - Reliance on hypervisors
  - Process isolation / Application sandboxes

4. Cloud support services

- **Advantages**
  - On demand security controls (e.g., authentication, logging, firewalls)

- **Challenges**
  - Additional risk when integrated with customer applications
  - Needs certification and accreditation as a separate application
  - Code updates

5. Cloud network and perimeter security

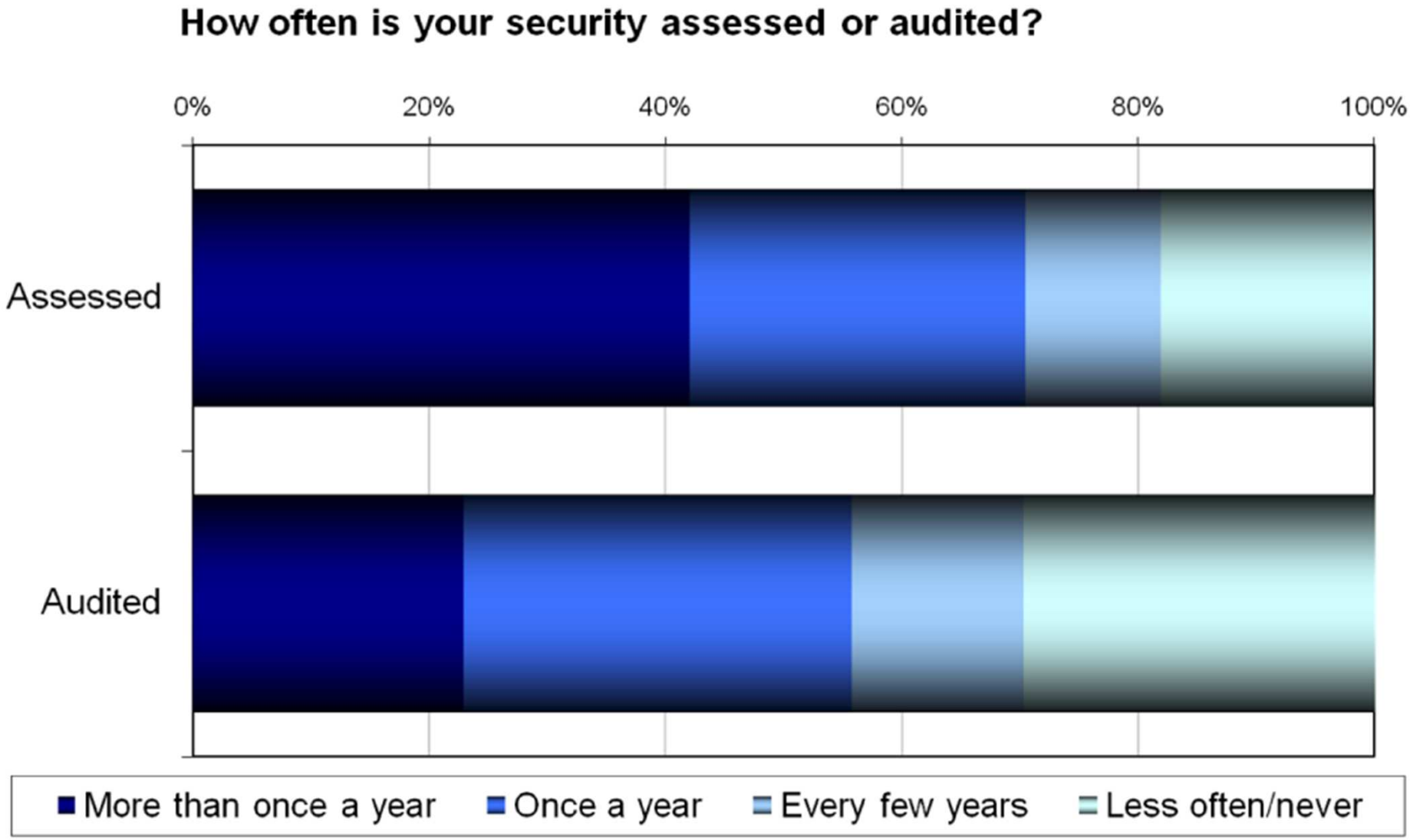
- **Advantages**
  - Distributed denial of service protection
  - VLAN capabilities
  - Perimeter security (IDS, firewall, authentication)

- **Challenges**
  - Virtual zoning with application mobility

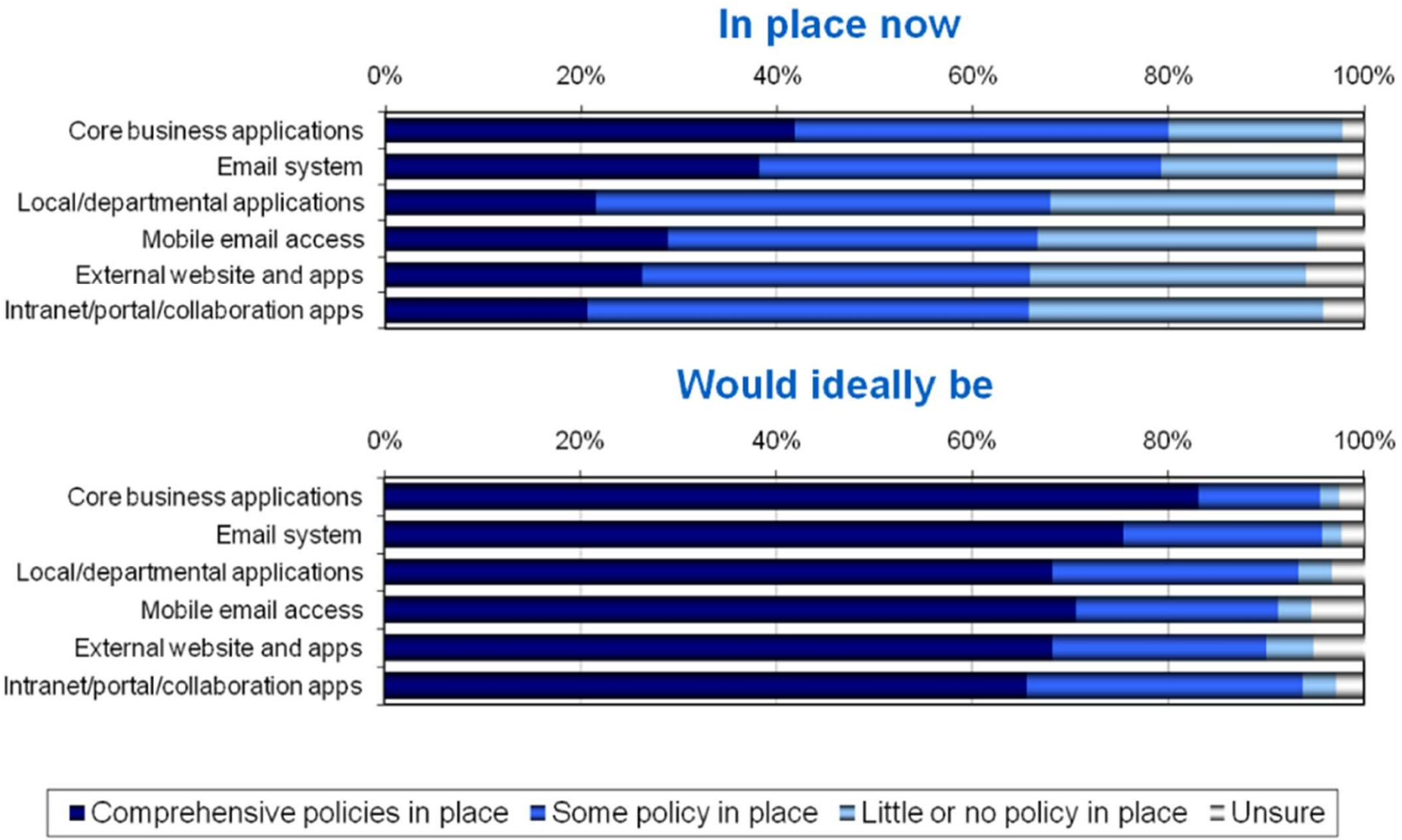
Other issues about “rule-compliance”

- Security issues
- Privacy issues (and risk of abuses)
- Compliance to IT standards (e.g., ISO, ITIL, PCI, SOX)
- **Which national legislation can be applied in an intrinsically super-national system, such as a Cloud infrastructure**

Is security in your data center adequate to your expectation? [Forrester research]

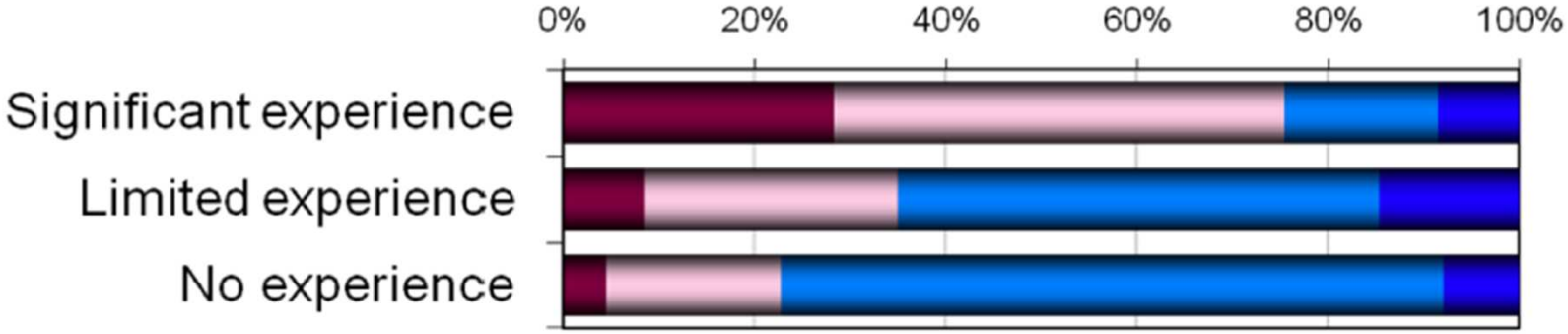


Security policies?

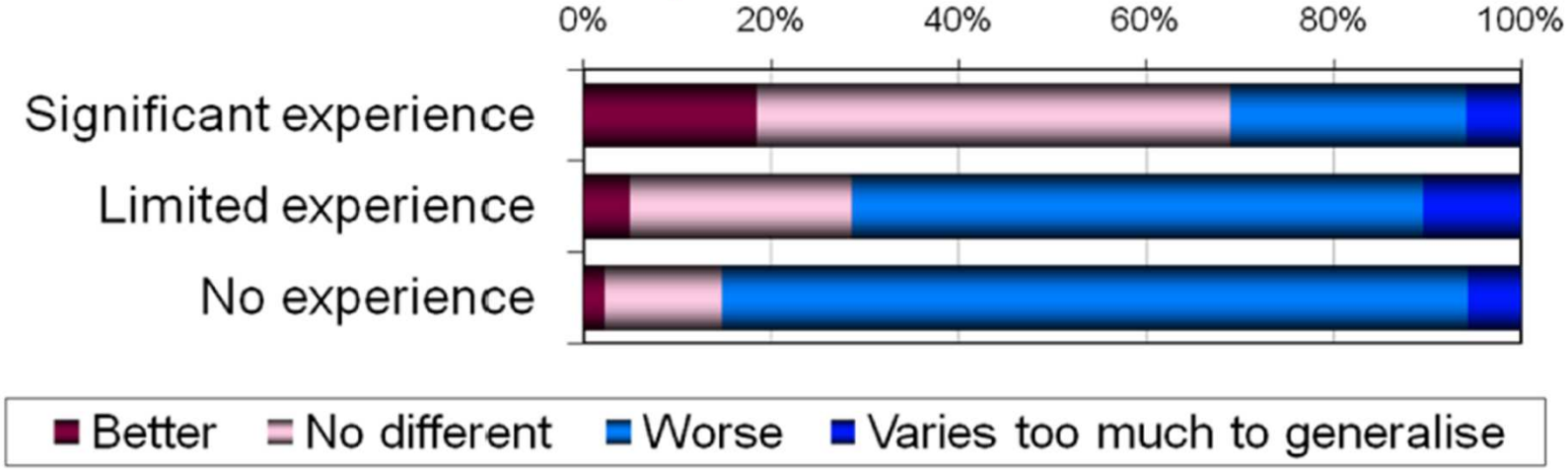


Security and privacy: opinions

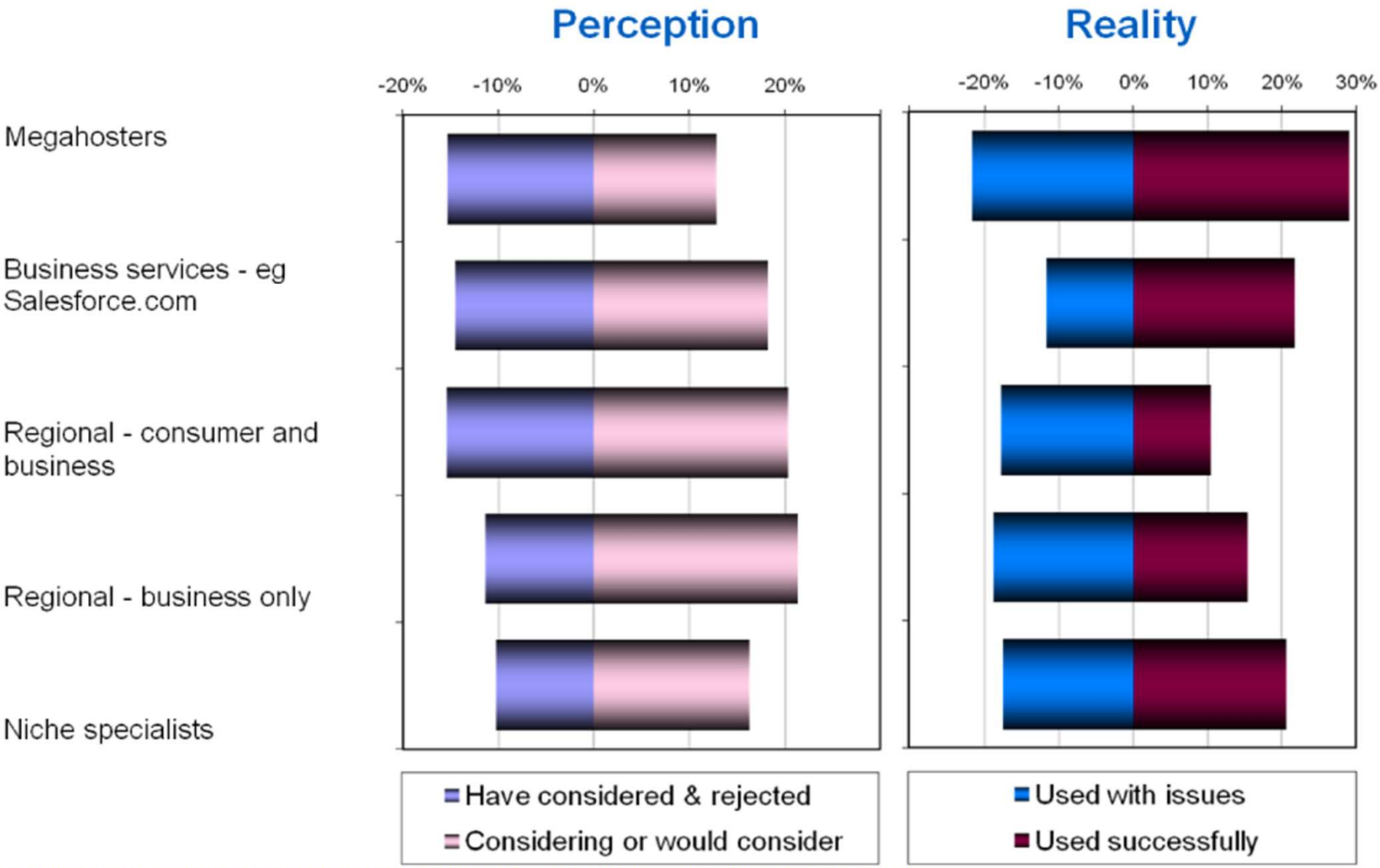
Security: SaaS better or worse than on-premise?



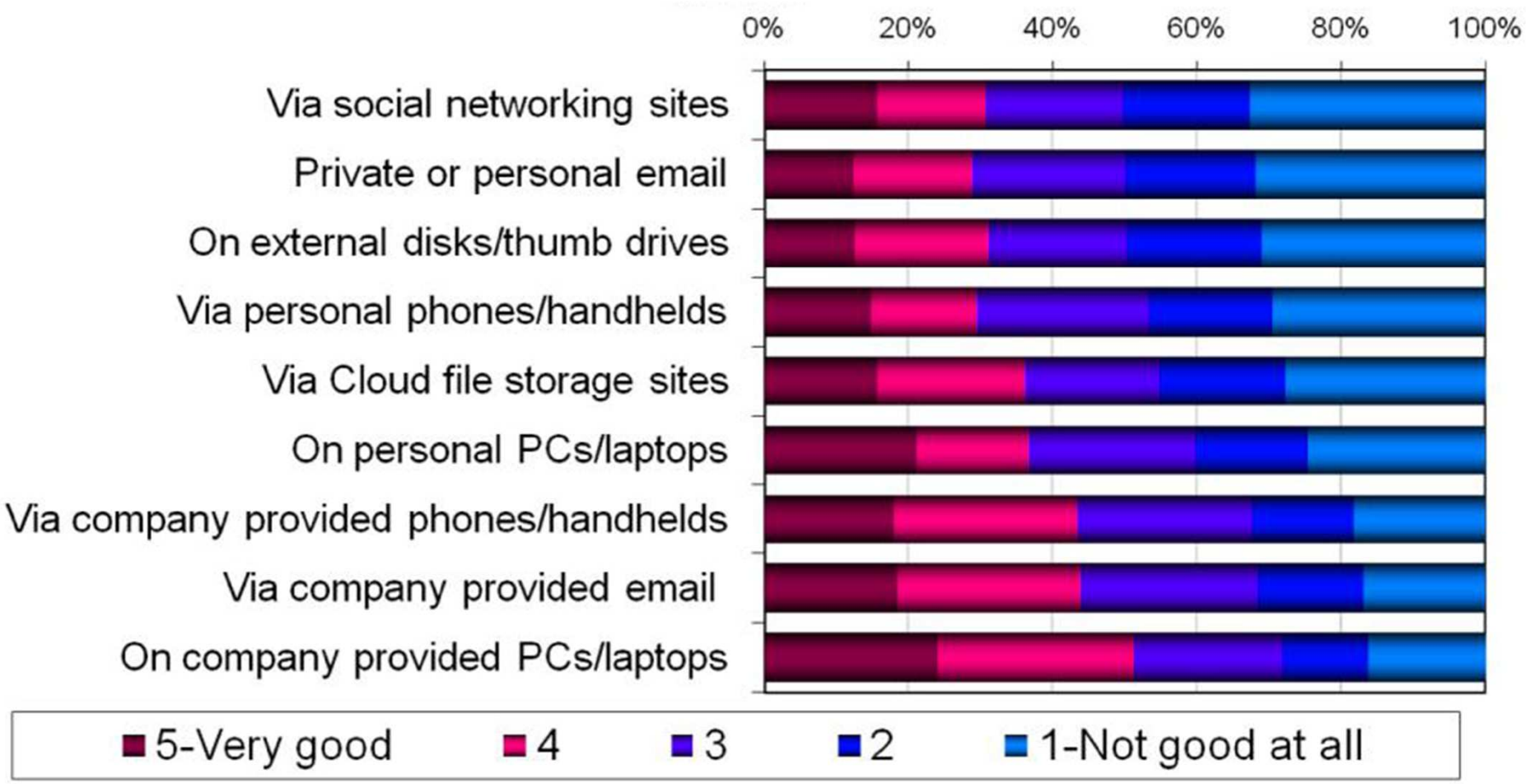
Privacy: SaaS better or worse than on-premise?



Perception and Reality



Data loss control?



Reality: A Cloud provider

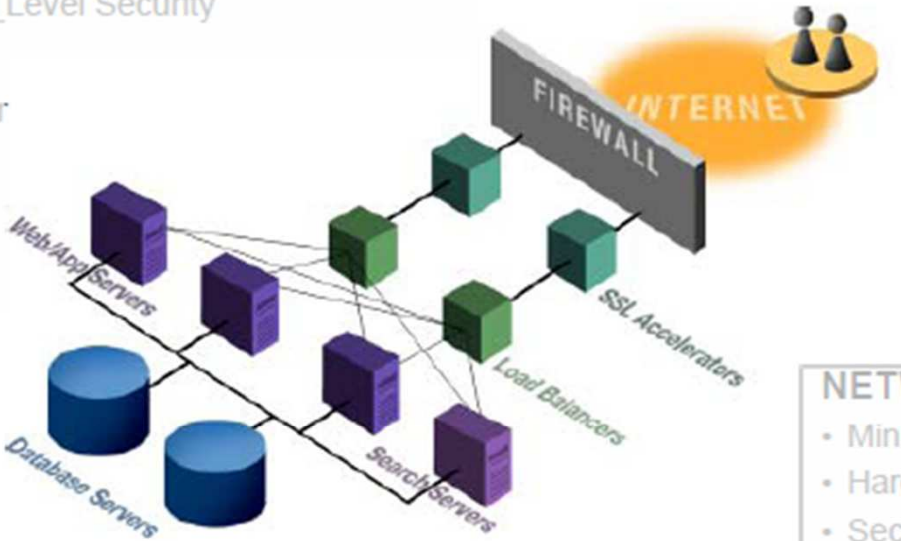
- Strong committment on security
- Analysis of employees (past records and way of conduct, including strong logging)
- Security team: 100+ experts
- Integrated security
  - Physical (24/7, electronic and biometric accesses, CCTV, multiple generators)
  - Continuous monitoring of threats and vulnerabilities
  - Security embedded in the lifecycle software development
  - Auditing and assessment
  - Incident Response Teams
- Certifications: Safe Harbor, PCI, SAS70, FISMA, …

Multi-layer security architecture

USER
- Password Policies
- Access Restrictions
- Logon Audit Trail
- Comprehensive Data Sharing Model
- Field Level Security

INTERNET
- 128-bit SSL for every transaction
- Verisign Certificates

PHYSICAL
- Completely secure hosting center
- 24x7 on-site security guards
- Biometric access screening
- Escort controlled access



FIREWALL
- Tightly controlled perimeter firewalls
- Intrusion detection
- Proactive log monitoring

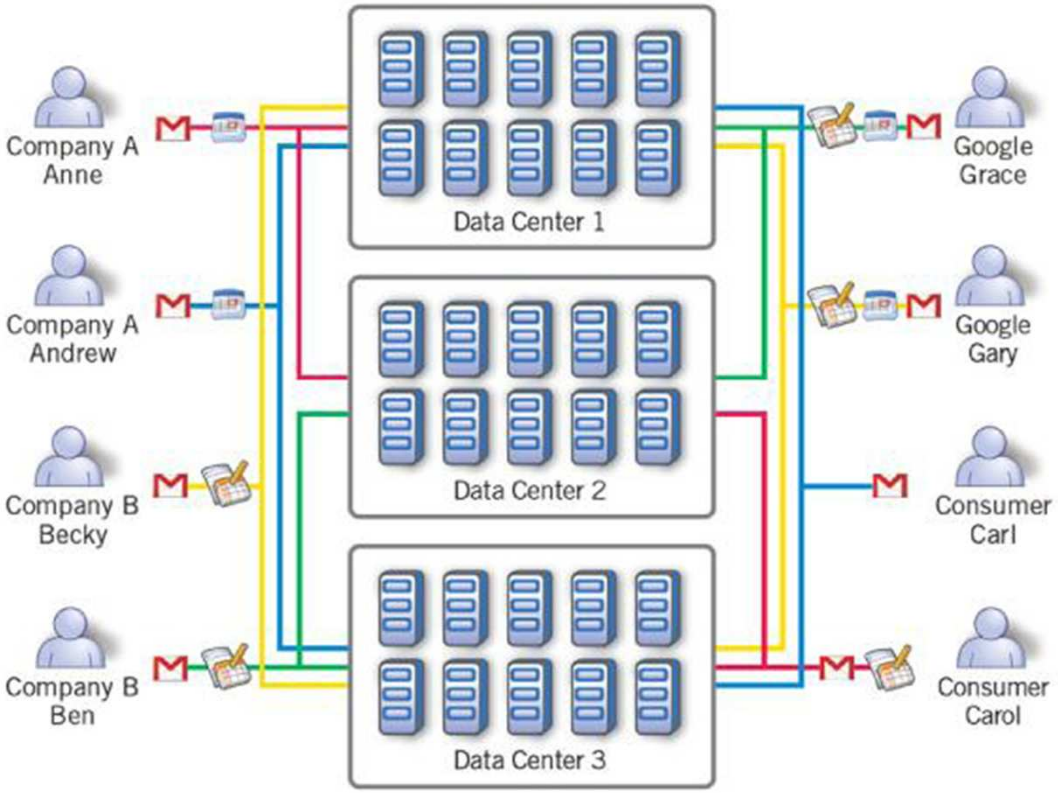
CORPORATE
- SFDC has no access to end-user passwords or rights to view your data

NETWORK / HOST
- Minimal routable IPs
- Hardened Operating Systems
- Secure Services

APPLICATION
- All passwords encrypted
- Highly secure session key management
- Multi-tenant Data Access Controls
- Application self-monitors for security violations

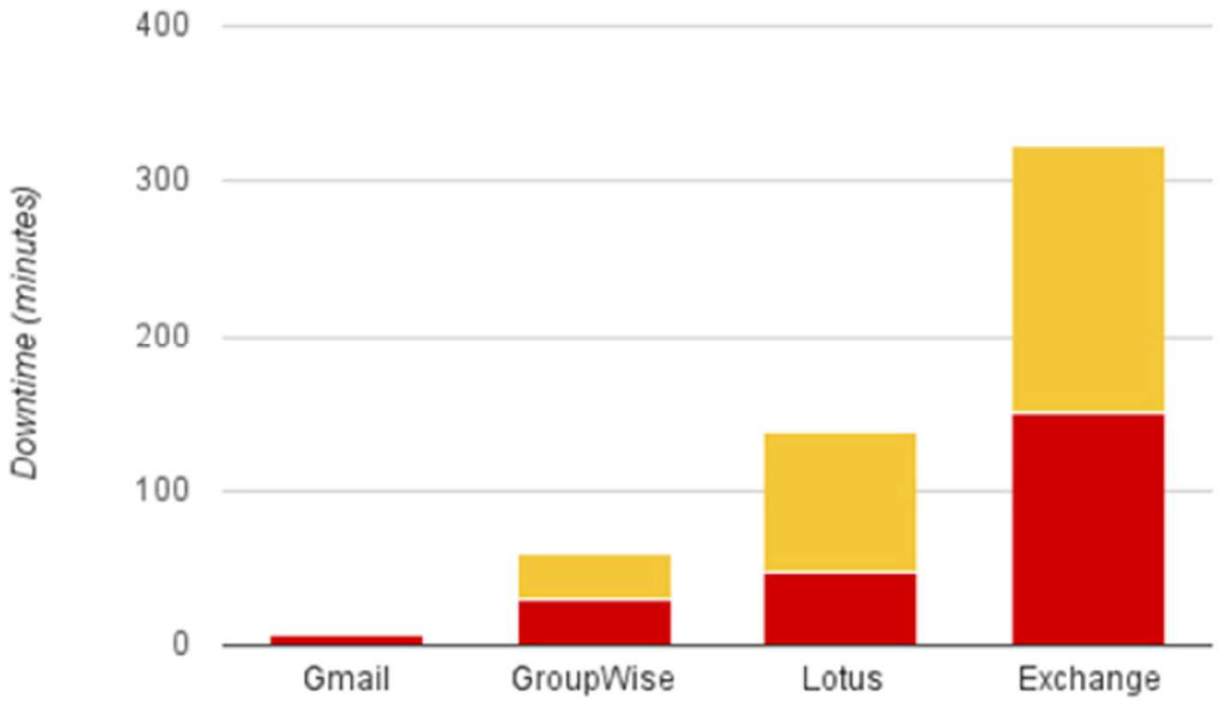
Privacy example: how Google stores data

- All data (Google, consumer, enterprise) in the same locations
- Data leakage prevention:
  - File separated in blocks and stored in different hosts
  - >100,000 blocks on the same disk
  - Random names for files with no relation with content
  - Data obfuscation



Cloud reliability

- Gmail: 99,984%
- 32X more than company email systems



CONCLUSIONS

My favourite critical infrastructure

Not yet 100% mature

- We aren’t moving to the cloud… We have to improve the present cloud infrastructures in several ways
- Globalization
- Massive multi-tenancy
- Pressure on traditional organizational boundaries
- Challenges traditional thinking
  - How do we build standards?
  - How do we create architectures?
  - What is the ecosystem required to managed, operate, assess and audit cloud systems?

Security topics for the future

- Authentication
- Availability
- Backup and recovery
- Compliance
- Data analysis
- Data loss prevention
- Forensics
- Hardening (systems, networks, applications, humans)
- Integration
- Privacy
- Scalability
- Virtualization
- …

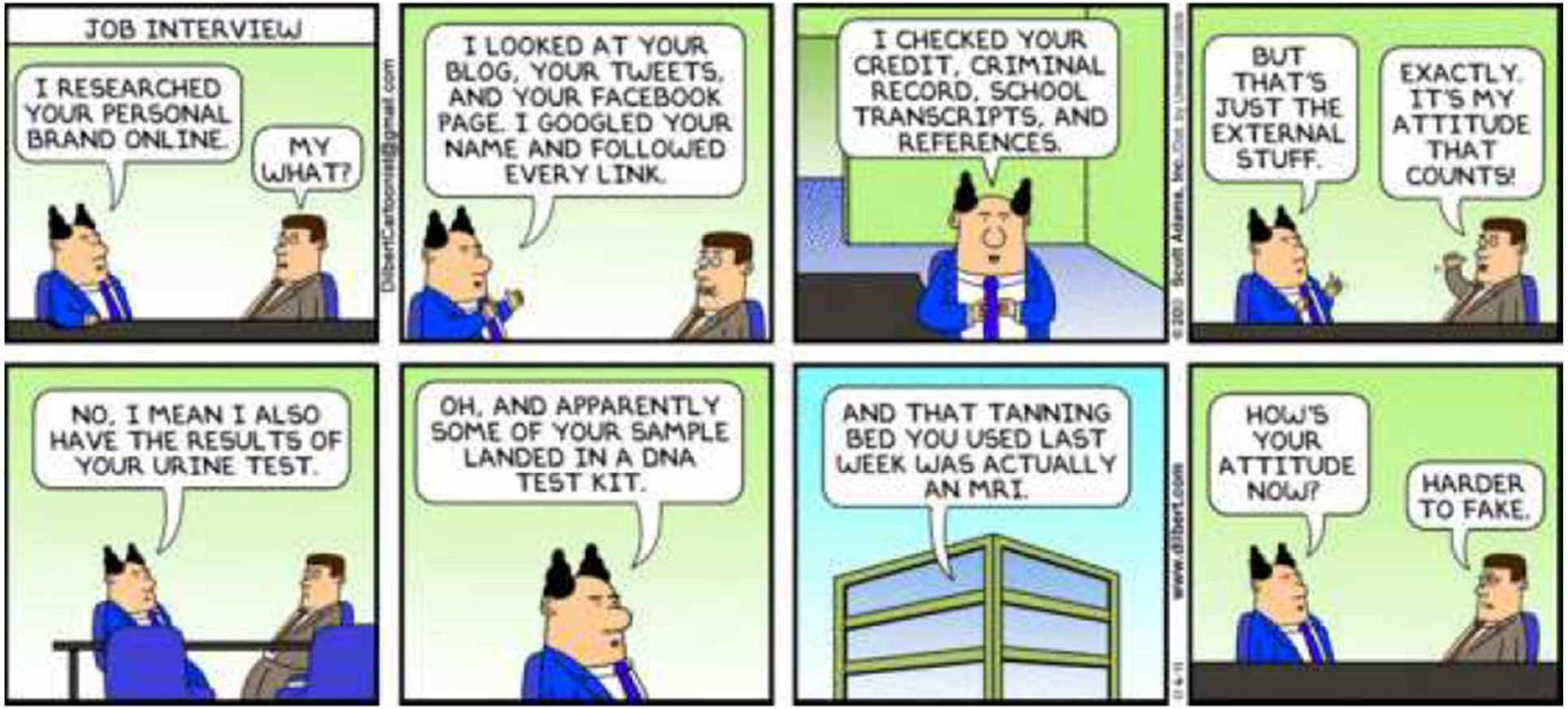
Same topics on a completely different scale for IT traditional services

***Same topics on different contexts* (e.g., P+I world)**

One of the goal

To get useful information from continuous data streams in order to take “adequate” decisions within real-time constraints

Not covered: *Security and privacy*



Not covered: *Data Loss Prevention* and *Internal attackers*

Chinese proverb

“*May you live in interesting times*”

Q & A

email: michele.colajanni@unimore.it

home page: *Google*(Michele Colajanni)