CYBER SECURITY, TRENDS & ANSWERS FOR CRITICAL NETWORK INFRASTRUCTURE

November 2011 – Timo Bakker, Director Public Sector Solutions

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

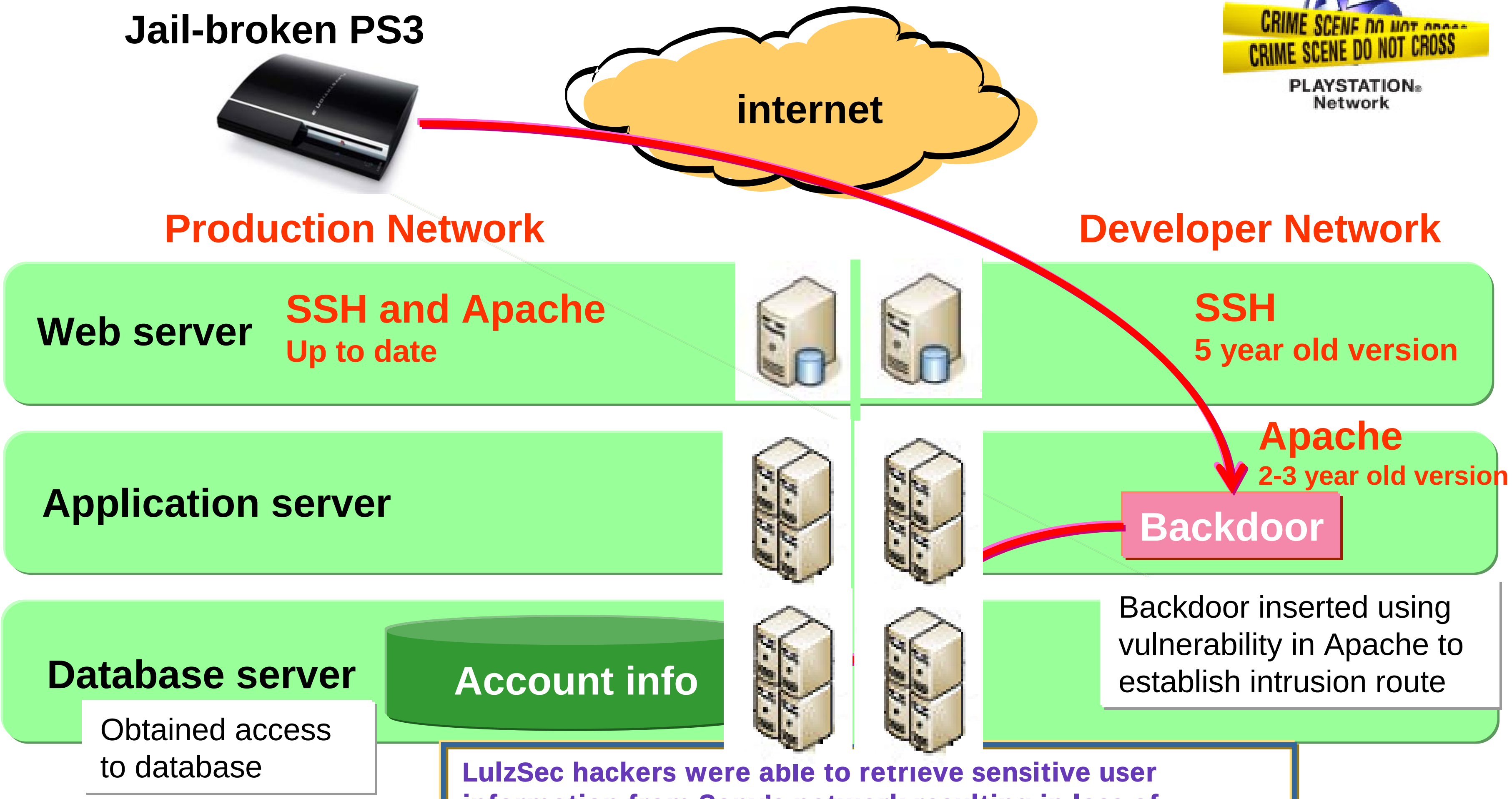
TRENDS IN CYBERCRIME, A NEW BATTLEFIELD….

What's happening out there ?

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

SONY PLAYSTATION NETWORK ATTACK

Probable Attack Vector

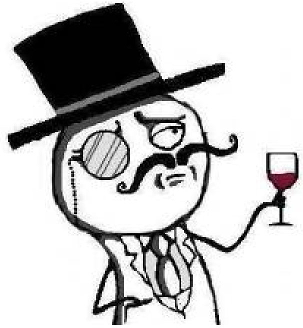


Backdoor inserted using vulnerability in Apache to establish intrusion route

Obtained access to database

LulzSec hackers were able to retrieve sensitive user information from Sony's network resulting in loss of reputation and 172 Mio US Dollar of revenue

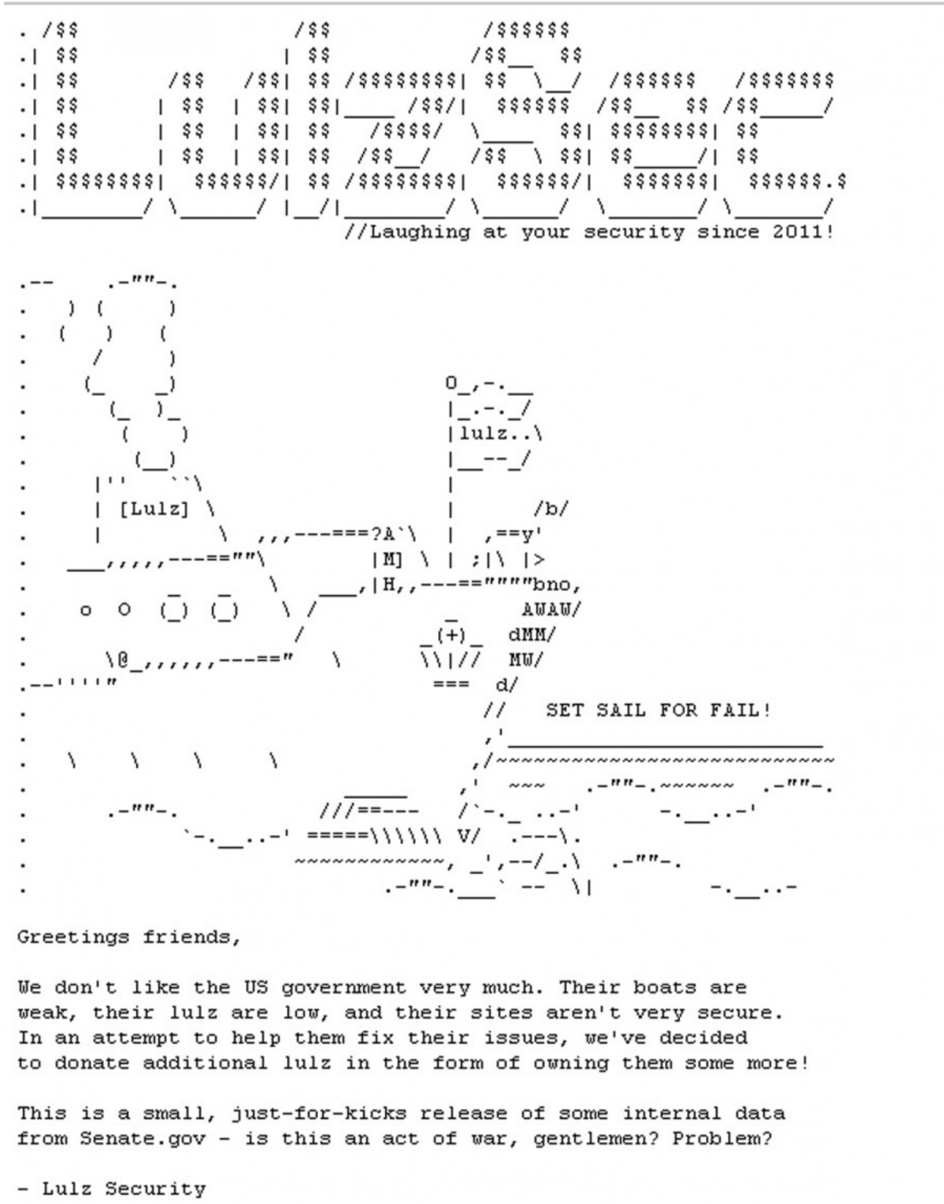
COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION



Logo of LulzSec

Lulz*Security, commonly abbreviated as **LulzSec**, is a computer hacker group that claims responsibility for several high profile attacks, such as the compromise of user accounts from Sony Pictures and taking the CIA website offline mid 2011.

The group is been described as a "cyber terrorism group"



```
. /$$                 /$$           /$$$$$$
.| $$                | $$          /$$__  $$
.| $$       /$$   /$$| $$ /$$$$$$$$| $$  \__/  /$$$$$$   /$$$$$$$
.| $$      | $$  | $$| $$|____ /$$/|  $$$$$$  /$$__  $$ /$$_____/
.| $$      | $$  | $$| $$   /$$$$/  \____  $$| $$$$$$$$| $$
.| $$      | $$  | $$| $$  /$$__/   /$$  \ $$| $$_____/| $$
.| $$$$$$$$|  $$$$$$/| $$ /$$$$$$$$|  $$$$$$/|  $$$$$$$|  $$$$$$.$
.|________/ \______/ |__/|________/ \______/  \_______/ \_______/
                          //Laughing at your security since 2011!

.--    .-""-.
.   ) (     )
.  (   )   (
.     /     )
.    (_    _)                     O_,-.__
.      (_  )_                     |_.-._/
.       (    )                    |lulz..\
.        (__)                     |__--_/
.     |''   ``\                   |
.     | [Lulz] \                  |      /b/
.     |         \  ,,,---===?A`\  |  ,==y'
.   ___,,,,,---==""\        |M] \ | ;|\ |>
.           _   _   \   ___,|H,,---==""""bno,
.    o  O  (_) (_)   \ /          _     AWAW/
.                     /         _(+)_  dMM/
.      \@_,,,,,,---=="   \      \\|//  MW/
.--''''"                         ===  d/
.                                    //   SET SAIL FOR FAIL!
.                                    ,'_________________________
.   \    \    \     \               ,/~~~~~~~~~~~~~~~~~~~~~~~~~~~
.                         _____    ,'  ~~~   .-""-.~~~~~~  .-""-.
.      .-""-.           ///==---   /`-._ ..-'      -.__..-'
.            `-.__..-' =====\\\\\\ V/  .---\.
.                     ~~~~~~~~~~~~, _',--/_.\  .-""-.
.                            .-""-.___` --  \|         -.__..-

Greetings friends,

We don't like the US government very much. Their boats are
weak, their lulz are low, and their sites aren't very secure.
In an attempt to help them fix their issues, we've decided
to donate additional lulz in the form of owning them some more!

This is a small, just-for-kicks release of some internal data
from Senate.gov - is this an act of war, gentlemen? Problem?

- Lulz Security
```

* Lulz = for a good reason, anything disturbing, do something offensive

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

WHAT HAVE THE CYBER CRIMINALS IN COMMON ?

Opportunity

Motive

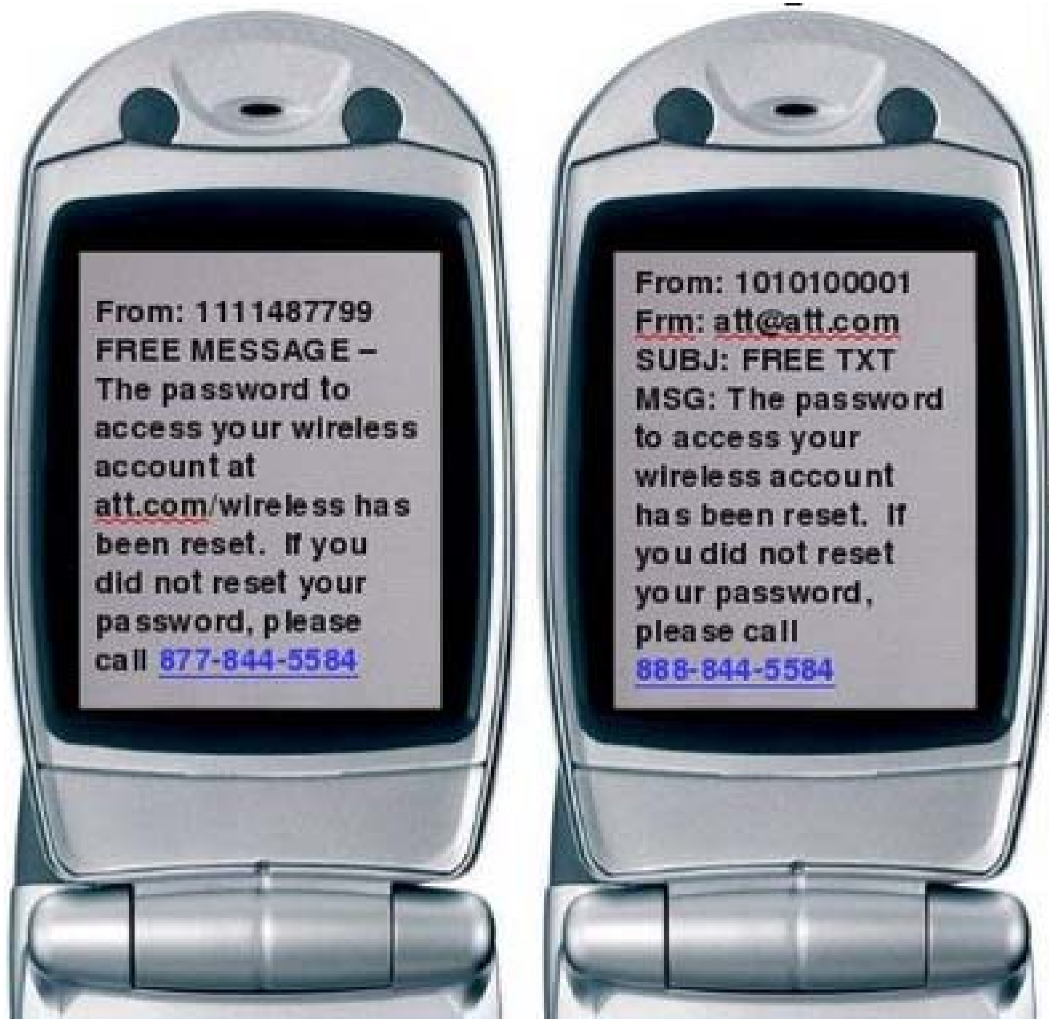
Capability

NEXT SLIDES WILL SHOW AN OPPORTUNITY APPROACH

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

WHICH MESSAGE IS THE LEGITIMATE MESSAGE?

2006



From: 1111487799
FREE MESSAGE –
The password to access your wireless account at att.com/wireless has been reset. If you did not reset your password, please call 877-844-5584

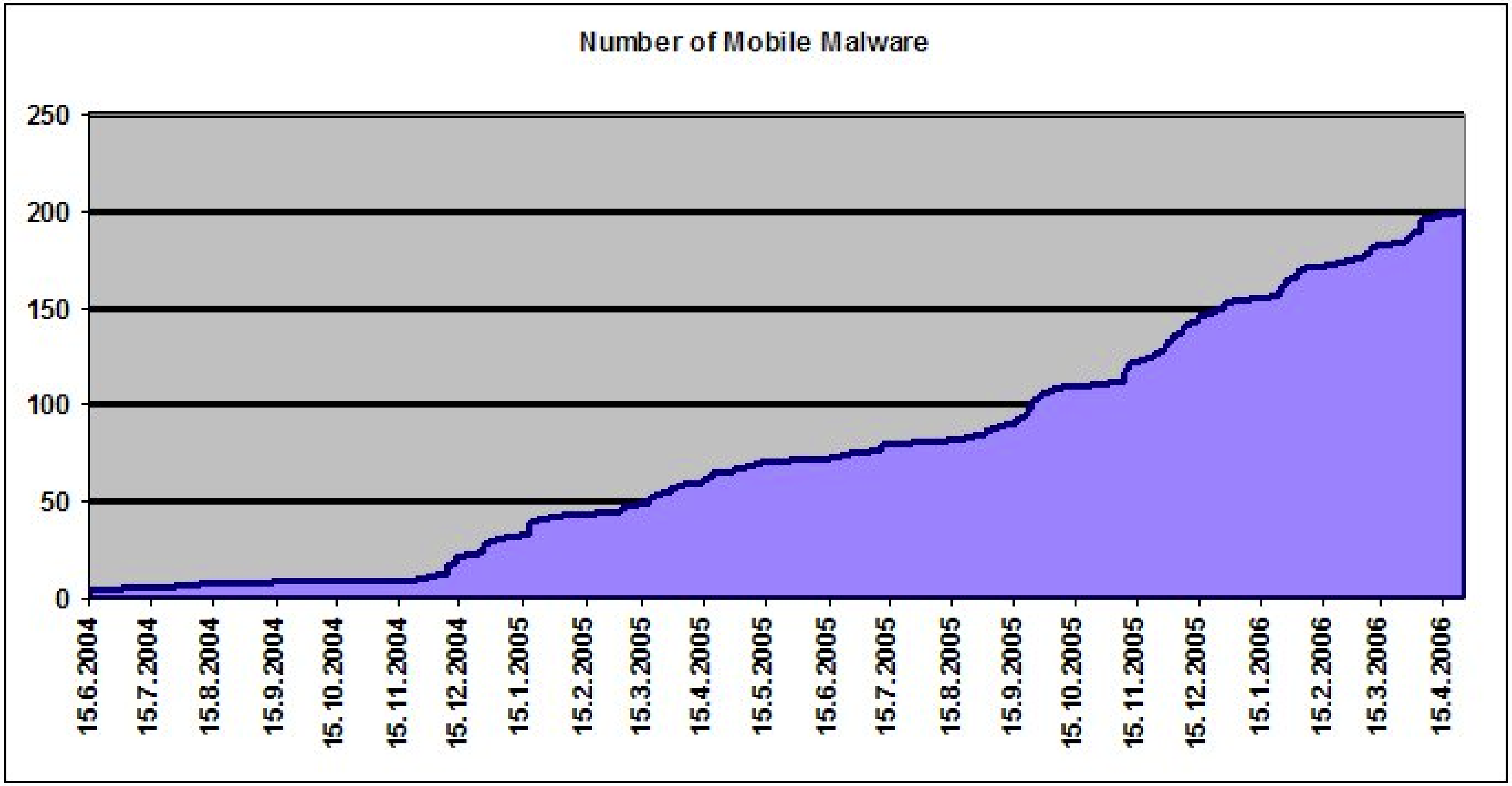
From: 1010100001
Frm: att@att.com
SUBJ: FREE TXT
MSG: The password to access your wireless account has been reset. If you did not reset your password, please call 888-844-5584

The one on the left is the real message. The other message is a spoofed message, sent using an open mail relay. This SMS spoofing trick no longer works on most mobile carriers worldwide.

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

TREND IN MALWARE FOR MOBILE DEVICES 2004-2006…

Did you own a Smart Phone in 2006 ?

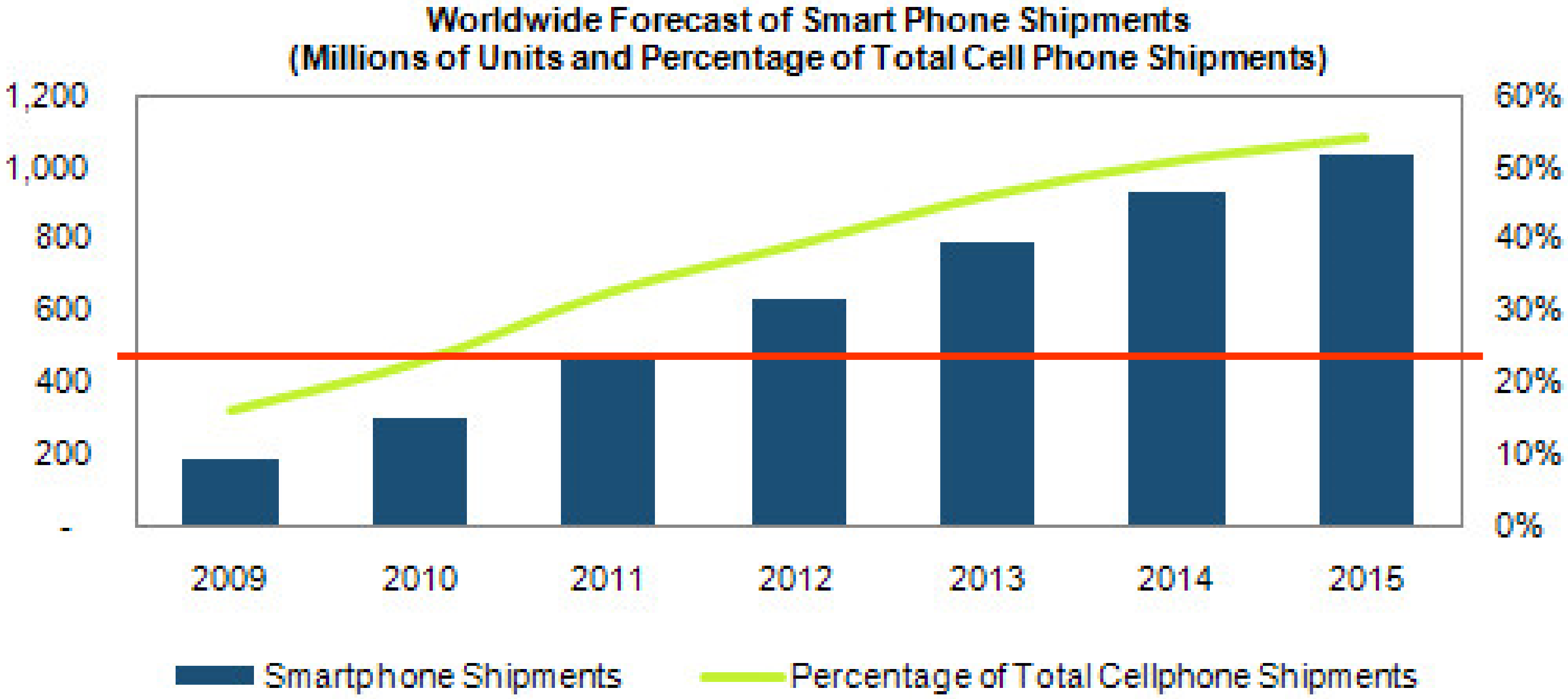


(Source: F-Secure)

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

SHIPMENT OF MOBILE SMART PHONES ...2009-2015

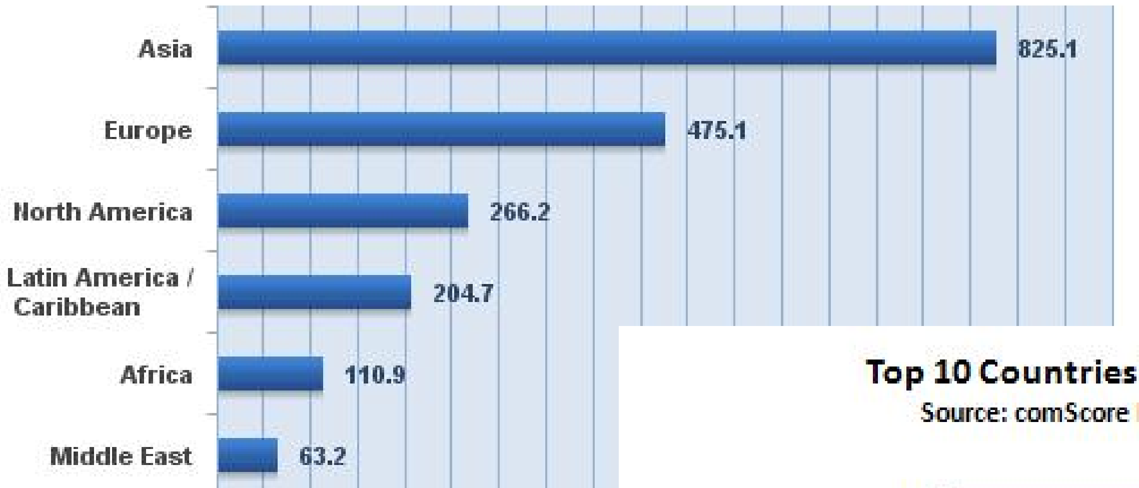
-



Source: IHS iSuppli August 2011

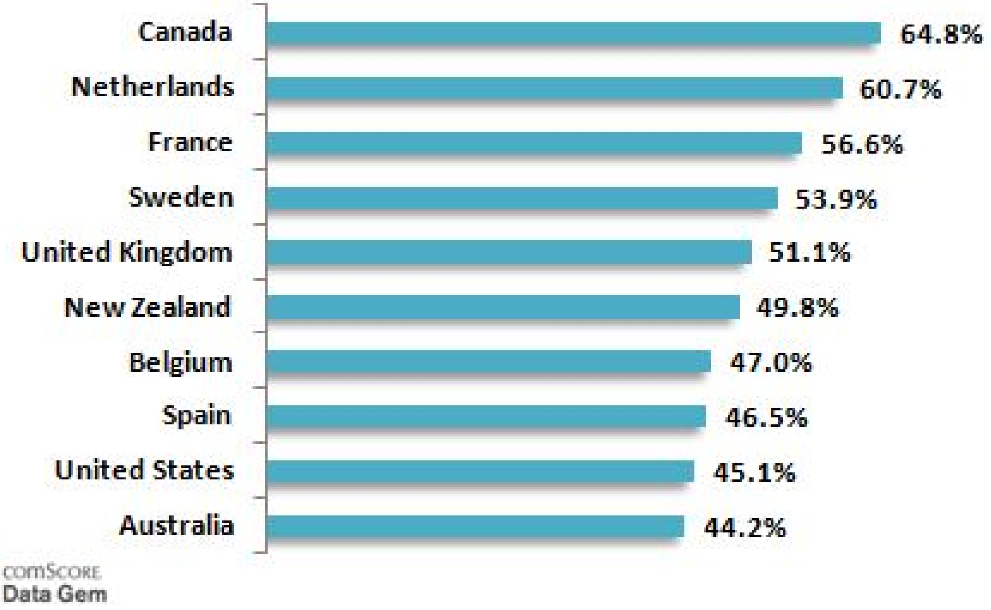
COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

Internet Users in the World by Geographic Regions - 2010



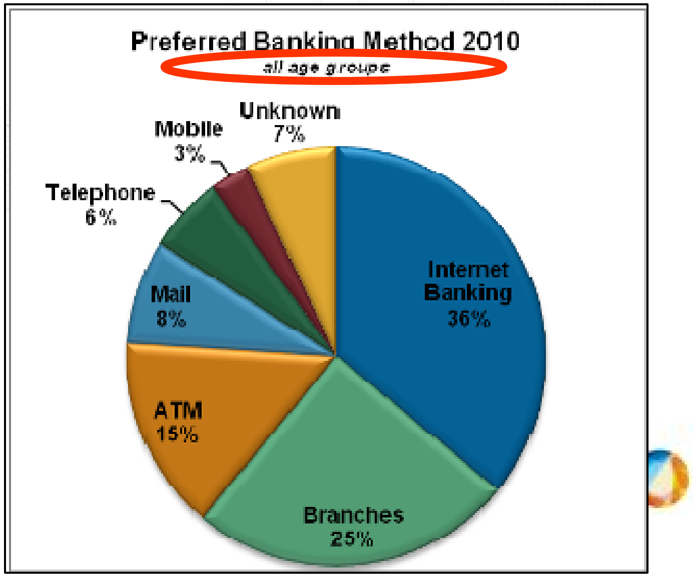
Top 10 Countries by Online Banking Penetration

Source: comScore Media Metrix, Age 15+, August 2010



comScore Data Gem

Preferred Banking Method 2010

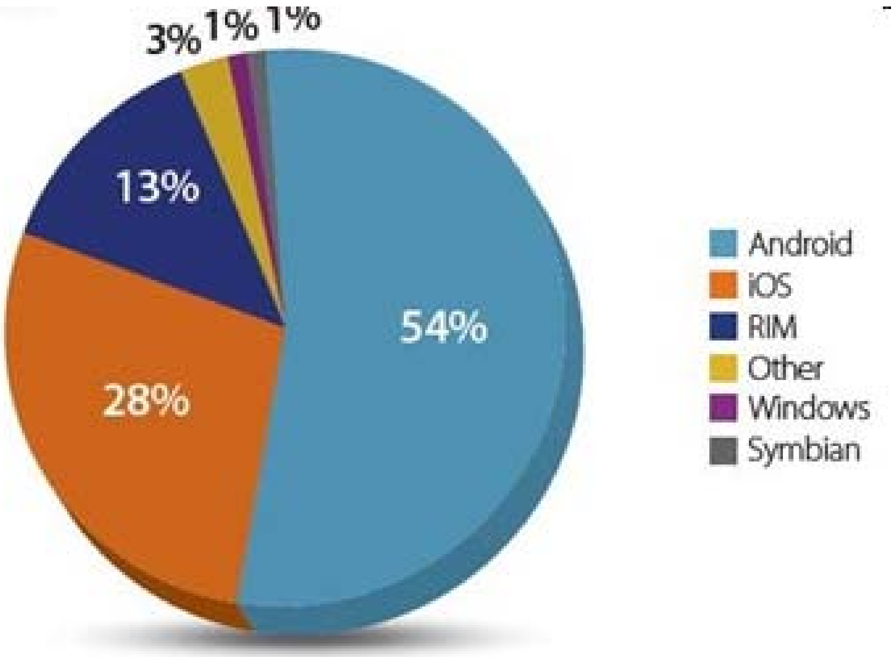


COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

GLOBAL MOBILE MALWARE TARGET PLATFORMS 2011

Android attacks have increased by 238% since Dec 2010. Android has emerged as the platform experiencing the largest number of new attacks.

Source: McAfee Labs Aug 2011



Source: Millennial Media, 8/11.
Other includes webOS, Danger, Nokia OS, Palm OS.

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

REAL TIME CYBER WAR & MOBILITY

EXAMPLES

DrdDream
- 1st major Trojan embedded in app
- 50+ apps removed from Android Market
- **Steals information and waits for instructions from C&C server**

Zeus
- **Targeting banks using mTAN authentication**
- Used against major Spanish institution
- Signed app for BB, WM, Symbian S60

09Droid
- Not malware but fake banking apps sold at $1.49
- Linking to bank’s own web site
- **Apps targeted 35 banks of all sizes**

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

REAL TIME CYBER WAR & MOBILITY
EXAMPLES

GoldDream.A

- Trojan: Logs incoming SMS' and outgoing calls,uploads them to an external server
- **Able to perform commands from the external server**
- Signed app for Android

NickiSpy

- Trojan—records the user's telephone conversations and stores them in the SD card memory
- **Monitors the user location and sends SMS to premium number**

Others:
Ikee, and Zitmo

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

THE MOBILE INFRASTRUCTURE CHALLENGE

- Mobile devices make use of different networks
- Often legacy systems, often without a homogeneous and/or secured configuration
- The default mobile encryption is weak and very easy to hack
- Even ONE single point attack can compromis the complete network connection and bring the network down

Cyber attacks target the critical infrastructure such as banks, utilities, transport networks, government networks and factories

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

EXPLOSIVE CYBER-ATTACK GROWTH

- **Denial of Service, Critical Network congestion**
- **Espionage (Trojan horse, traffic redirect, phishing emails..)**
- **Computer control taking, Worms designed to target critical infrastructure such as power stations, transport, industrial units…**

28% of enterprises recognized successful attacks & 44% of enterprises recognized misuses

"CSI/FBI Computer Crime and Security Survey, 2009"

20,000 malicious emails sent to government networks each month

"CSI/FBI Computer Crime and Security Survey, 2009"

"Cyber crime involves attacks on computer networks, impacting on anything from the national grid to hospital computers and online bank accounts. They can come from anywhere and be carried out by anyone with the know-how."
-- UK National Security Strategy, Oct'10

1st semester of 2010:

1896 new identified security weaknesses
100 new viruses for Mobile Phone
1 mail out of 119 is a phishing

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

ISRAEL: IDF, MOSSAD, BACK ONLINE AFTER DAY OF COMPUTER HACK

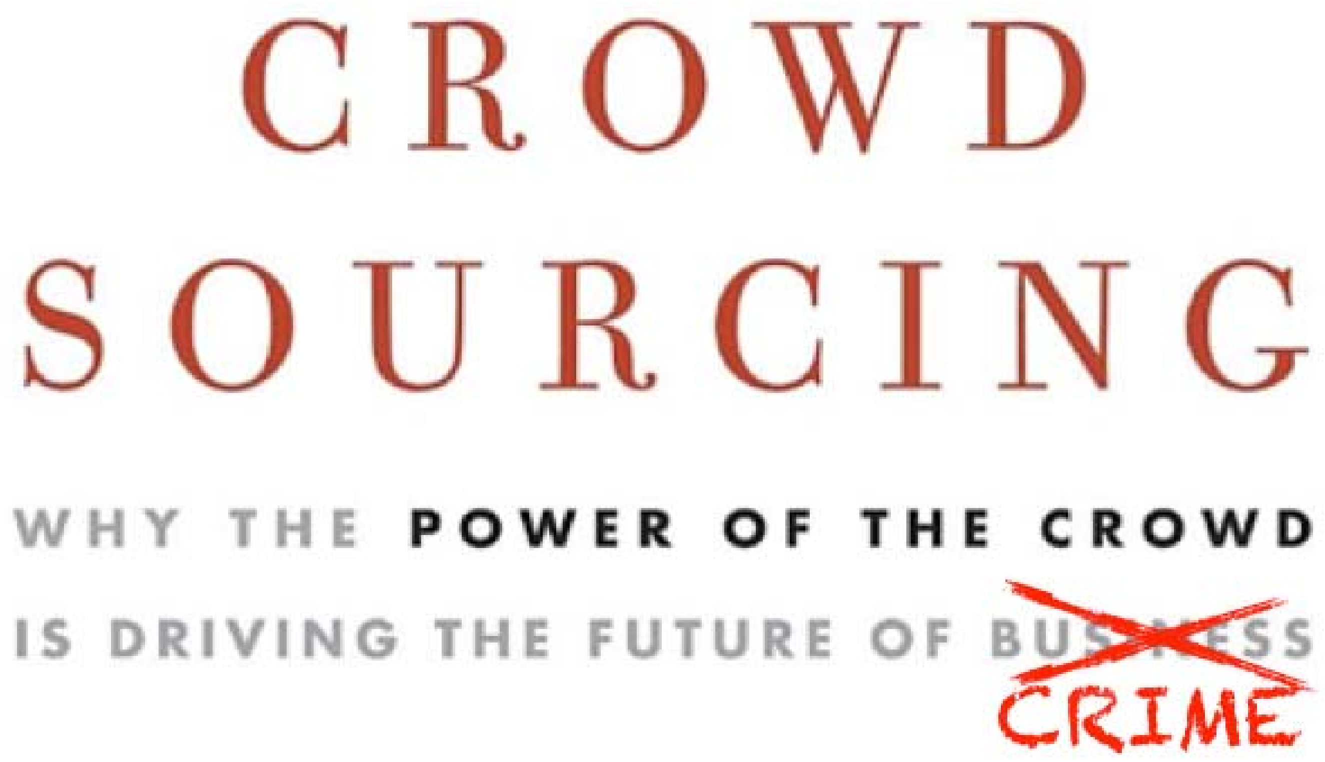
Logo of Anonymous Group

http://www.youtube.com/watch?v=QNxi2lV0UM0&feature=player_embedded
http://www.youtube.com/watch?feature=player_embedded&v=3ZL0E1J7wOg#!

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

CYBER CRIME 2.0

Borderless distributed ICT criminality



CROWD SOURCING

WHY THE POWER OF THE CROWD IS DRIVING THE FUTURE OF ~~BUSINESS~~ CRIME

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

CYBER CRIME 2.0

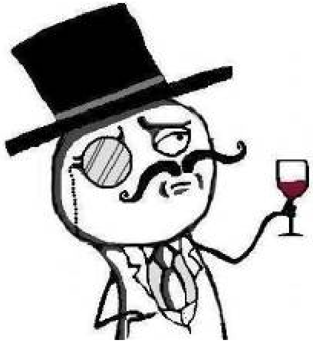
Crowdsourcing app for modern bank robbery

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

CYBER CRIME 2.0

The crime request hotline

NEW!



The online crime request

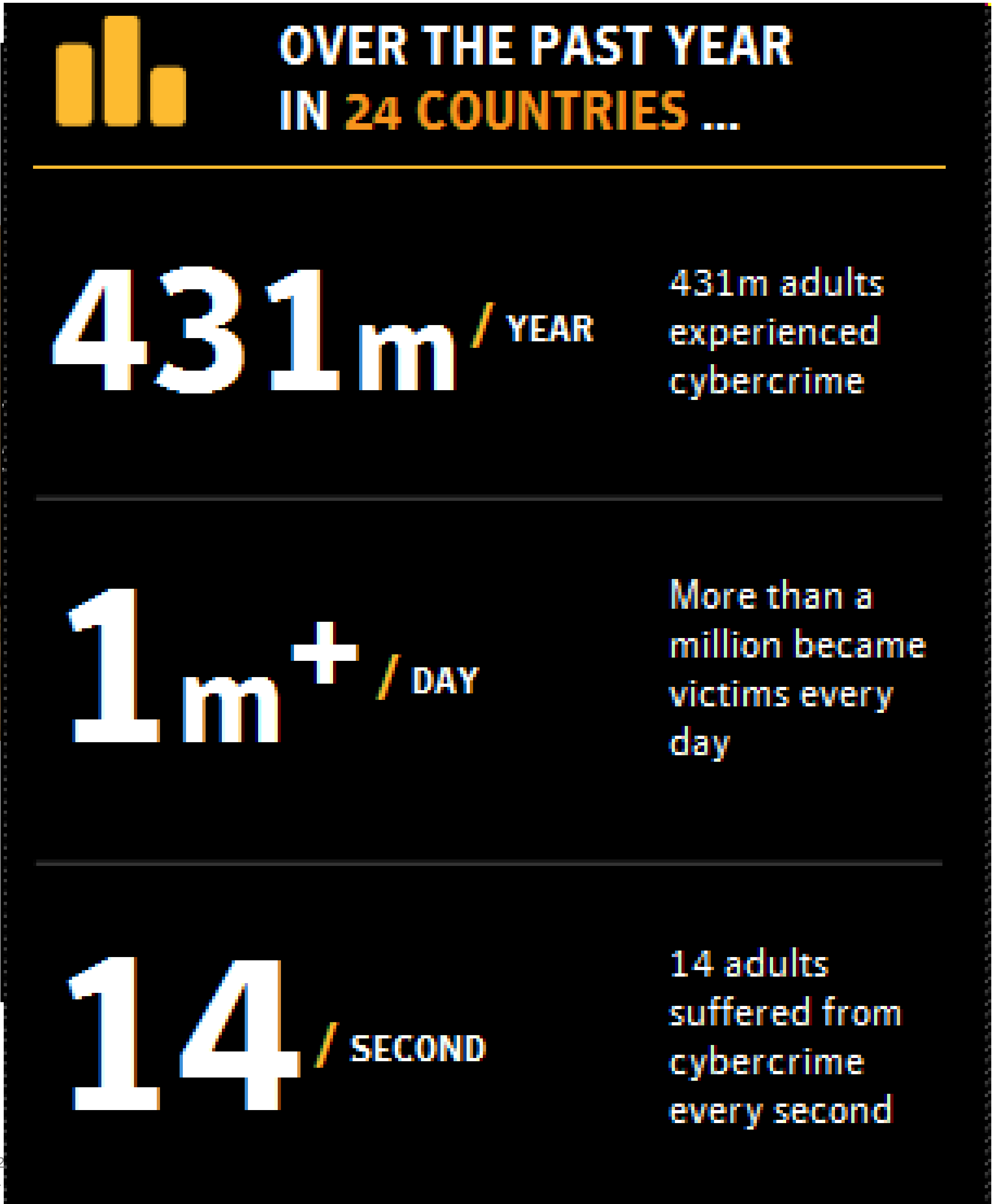
HOTLINE

Invented by LulzSec

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

OUTPERFORMER ILLEGAL DRUGS MARKET

This business office has
a yearly turnover of 250 Mio Euro



OVER THE PAST YEAR
IN 24 COUNTRIES ...

431m / YEAR

431m adults experienced cybercrime

1m+ / DAY

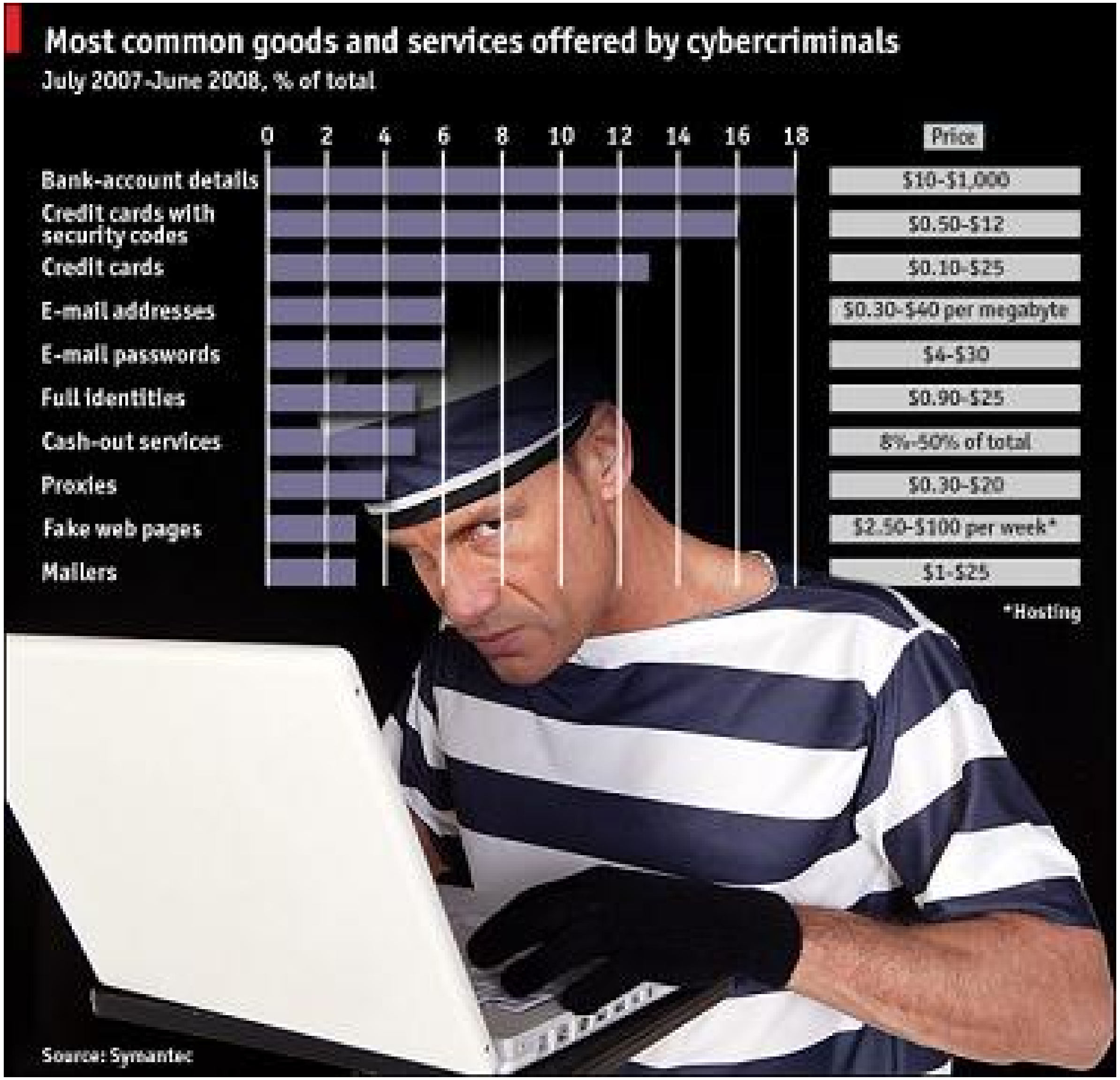
More than a million became victims every day

14 / SECOND

14 adults suffered from cybercrime every second

TOP 10 BEST SELLERS TO CYBER PIRATES ?

Market values



Most common goods and services offered by cybercriminals

July 2007-June 2008, % of total

	Price
Bank-account details	$10-$1,000
Credit cards with security codes	$0.50-$12
Credit cards	$0.10-$25
E-mail addresses	$0.30-$40 per megabyte
E-mail passwords	$4-$30
Full identities	$0.90-$25
Cash-out services	8%-50% of total
Proxies	$0.30-$20
Fake web pages	$2.50-$100 per week*
Mailers	$1-$25

*Hosting

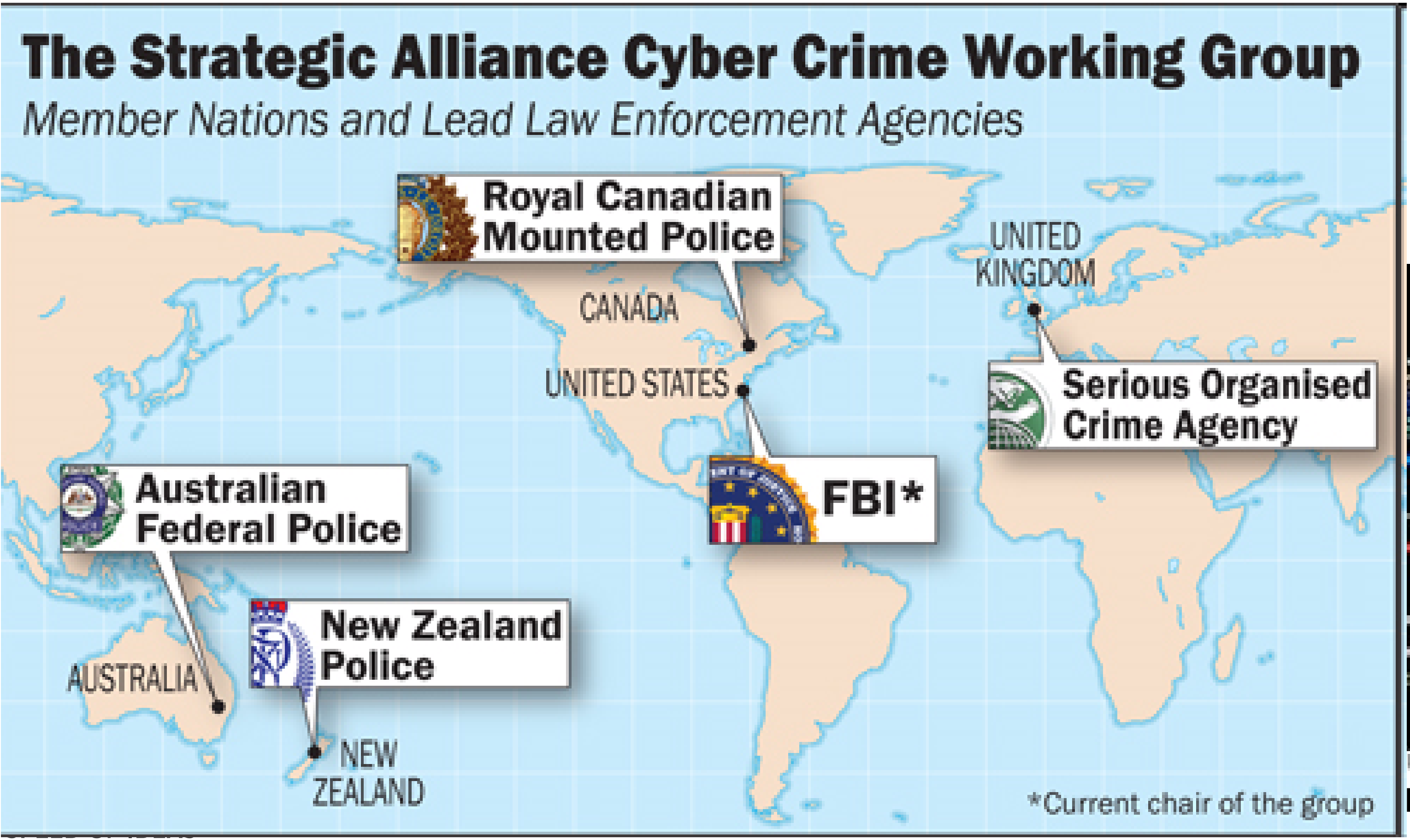
Source: Symantec

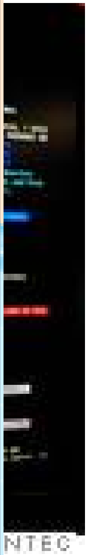
Source: Symantec

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

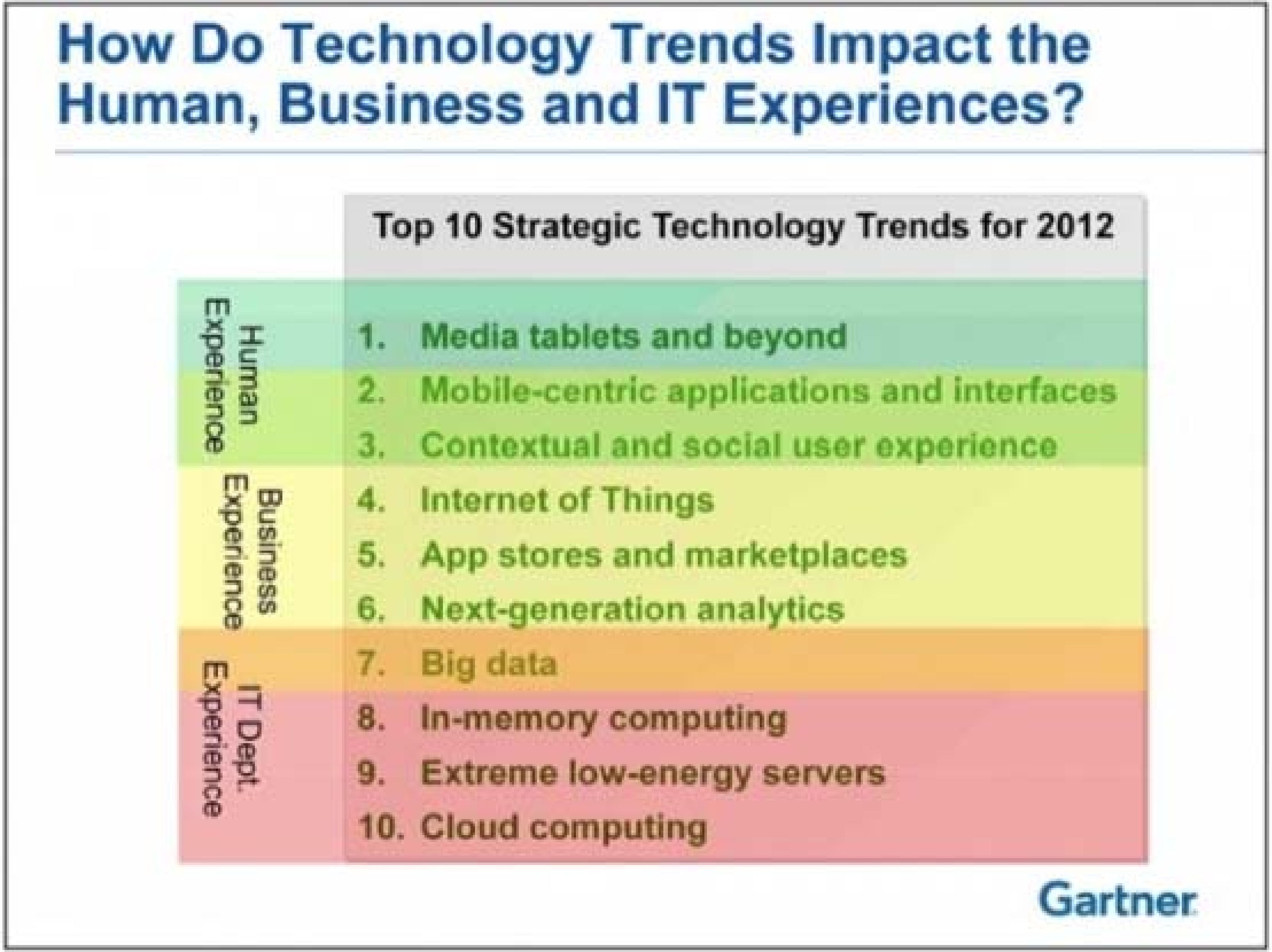
"Cyber will be part of any future conflict whether it's a nation, state or terrorism,"

Cofer Black, former director of the CIA's LasVegas August 2011.


The Strategic Alliance Cyber Crime Working Group
Member Nations and Lead Law Enforcement Agencies
Royal Canadian Mounted Police
CANADA
UNITED STATES
FBI*
UNITED KINGDOM
Serious Organised Crime Agency
Australian Federal Police
AUSTRALIA
New Zealand Police
NEW ZEALAND
*Current chair of the group



COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION



How Do Technology Trends Impact the Human, Business and IT Experiences?

	Top 10 Strategic Technology Trends for 2012
Human Experience	1. Media tablets and beyond
	2. Mobile-centric applications and interfaces
	3. Contextual and social user experience
Business Experience	4. Internet of Things
	5. App stores and marketplaces
	6. Next-generation analytics
IT Dept. Experience	7. Big data
	8. In-memory computing
	9. Extreme low-energy servers
	10. Cloud computing

Gartner

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

Where do we go from here?

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

DRIVE FOR CYBER SECURITY

Un-Constrained

capacity

Ubiquitous

everywhere

Un-tethered

wireless

Given un-constrained ubiquitous un-tethered global access, we have increased exposure to threats

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

DRIVE FOR CYBER SECURITY

Greater complexity: Convergence, Web 2.0+. Cloud, Big Data

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

CYBER-THREATS, CYBER-ATTACKS

MAJOR THREATS

INFORMATION DISCLOSURE

INFORMATION CORRUPTION

OPERATION DISRUPTION

CYBER-ENEMIES

UNCOORDINATED INDIVIDUALS

VIRTUAL or ORGANIZED GROUP

STATE-LED ACTIONS

CYBER-ATTACKS

PHYSICAL ATTACKS (HERF, AC destruction, electronic interception...)

SYSTEMS INTRUSION (backdoors, admin accounts...)

MALWARE (virus, worms, trojans, botnet...)

Networks are now major vehicle for cyber-attacks !

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

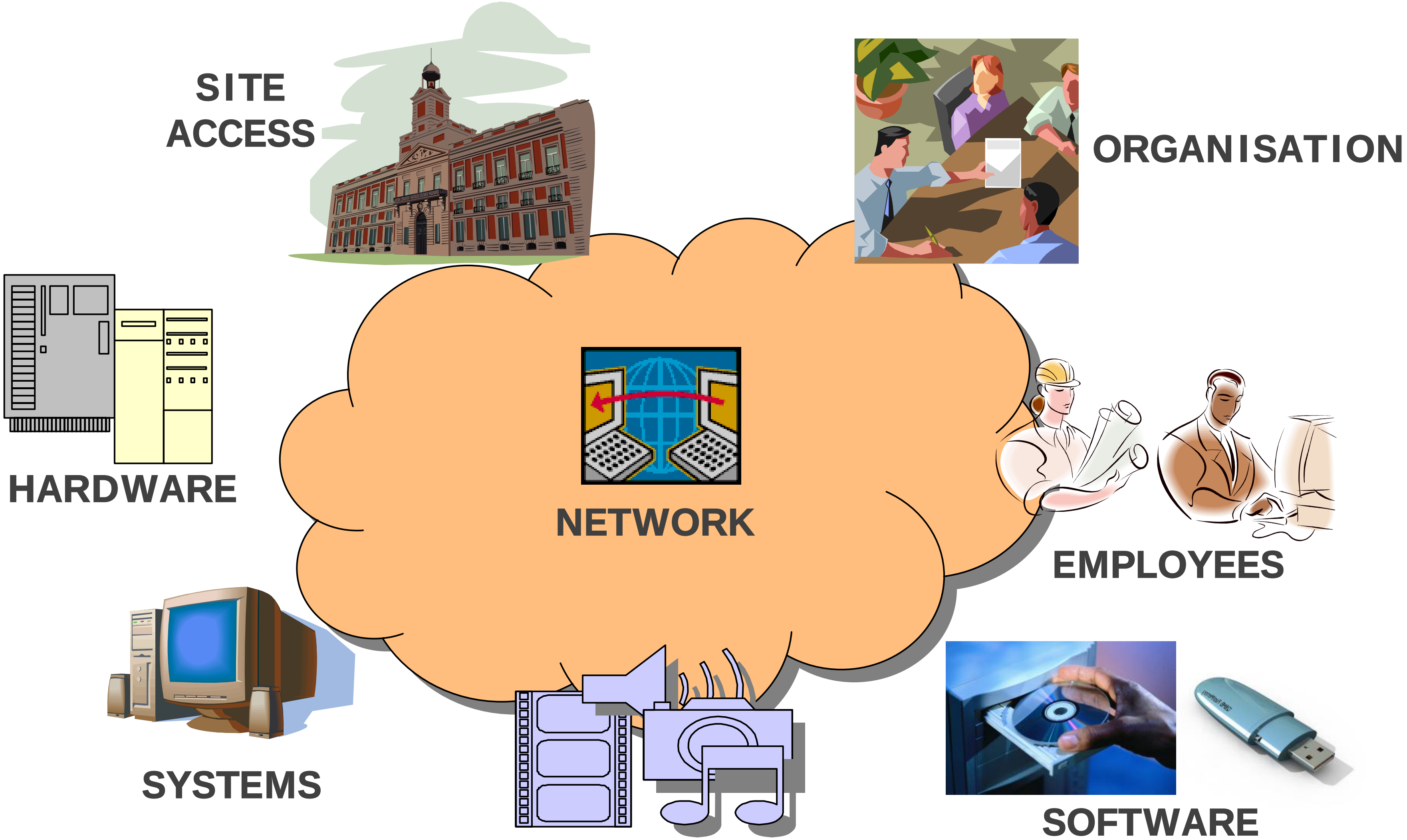
HOLISTIC SECURITY VIEW FOR NATIONAL CRITICAL INFRASTRUCTURES

- 5 Top Reasons to master your Information System security
  - **vulnerabilities** (and exploits) are found for the products you have deployed
  - No network is totally isolated hence you can get **hacked** or hit by **viruses** and the likes
  - Beware of **insiders** abuse
  - Customer's **organisation** and **systems** are **evolving** and changing
  - **Regulations and Legal Compliancy** require a **constant assessment** of the situation (**SOX, NERC, CIP, BASEL II**, ...)

> *" **Security** Is a **Process** Not a **Product**... Is Anyone Paying Attention?"* Bruce Schneier

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

CYBER-THREATS, CYBER-ATTACKS: IDENTIFYING VULNERABILITIES



SITE ACCESS

ORGANISATION

HARDWARE

NETWORK

EMPLOYEES

SYSTEMS

SOFTWARE

INFORMATION

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

HOW TO DEAL WITH CYBER-DEFENSE

A matter of structure, process, organization, technology and best practice sharing

Cyber-Defense Doctrine

Cyber policy? Offence and Defense?

How to apply ? How to control ? How to assess ?

How to take into account technology evolution ?

Technology & Security Capabilities

Must Have but How to be sure equipment are doing what they are supposed to do ? How to cope with required network upgrade ? How to securely integrate security solutions ?

How to practically implement Security Policy ? How to control? How to assess ? How to alert ?

Cyber-Defense team

Structure?

Competence acquisition and maintenance are expensive

Training ? How to control efficiency ? Collaboration ?

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

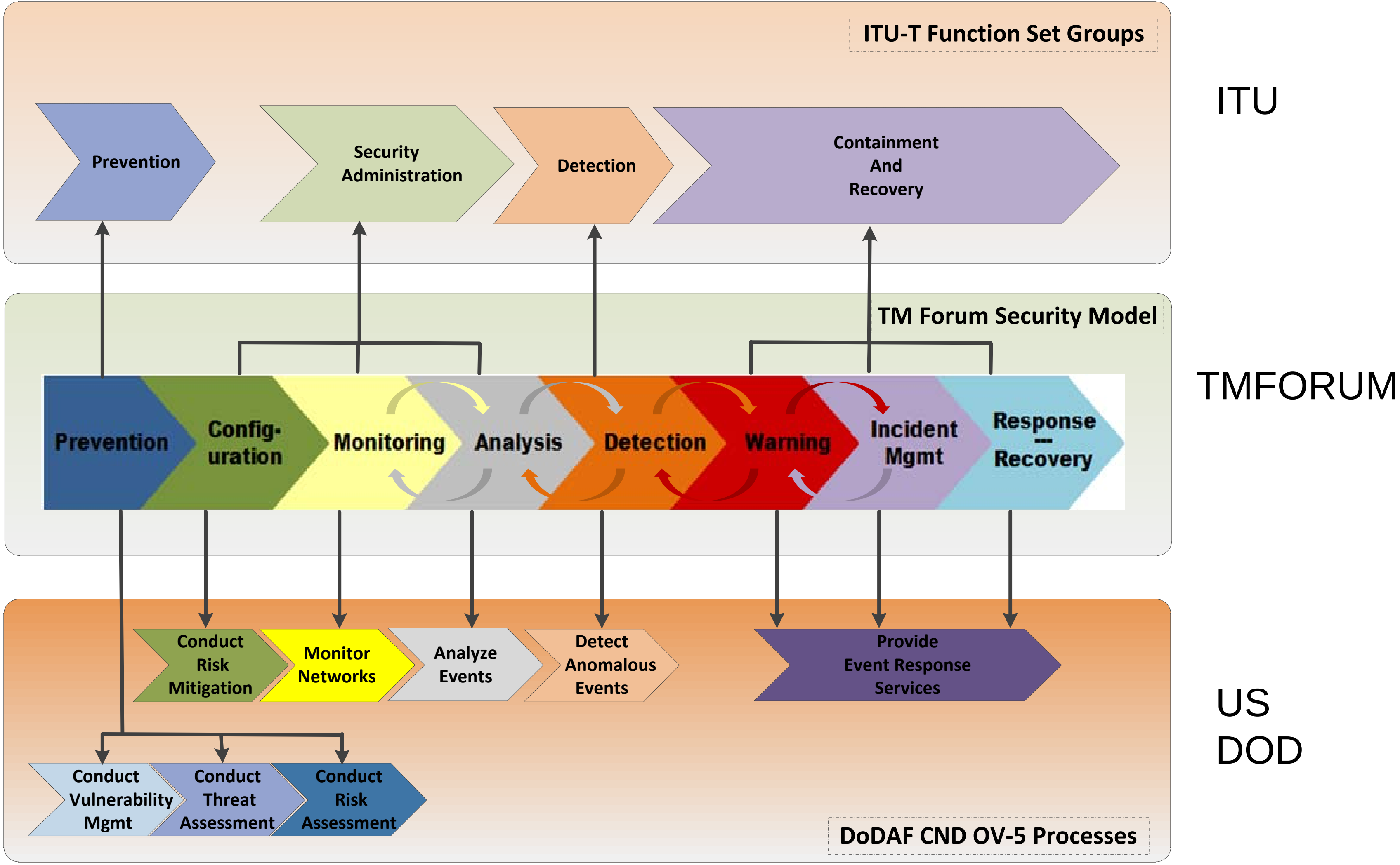
MAIN SECURITY FUNCTIONS & RELATED THREATS IN CRITICAL NETWORK INFRASTRUCTURE

Technical Security Goal	**General Threats**				
	Destruction	Corruption / Modification	Removal	Disclosure / Interception	Interruption
Authentication			🟩	🟩	
Access control	🟩	🟩	🟩	🟩	
Confidentiality			🟩	🟩	
Data Integrity	🟩	🟩			
Privacy				🟩	
Availability	🟩				🟩
Communication security			🟩	🟩	
Accountability	🟩	🟩	🟩	🟩	🟩

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

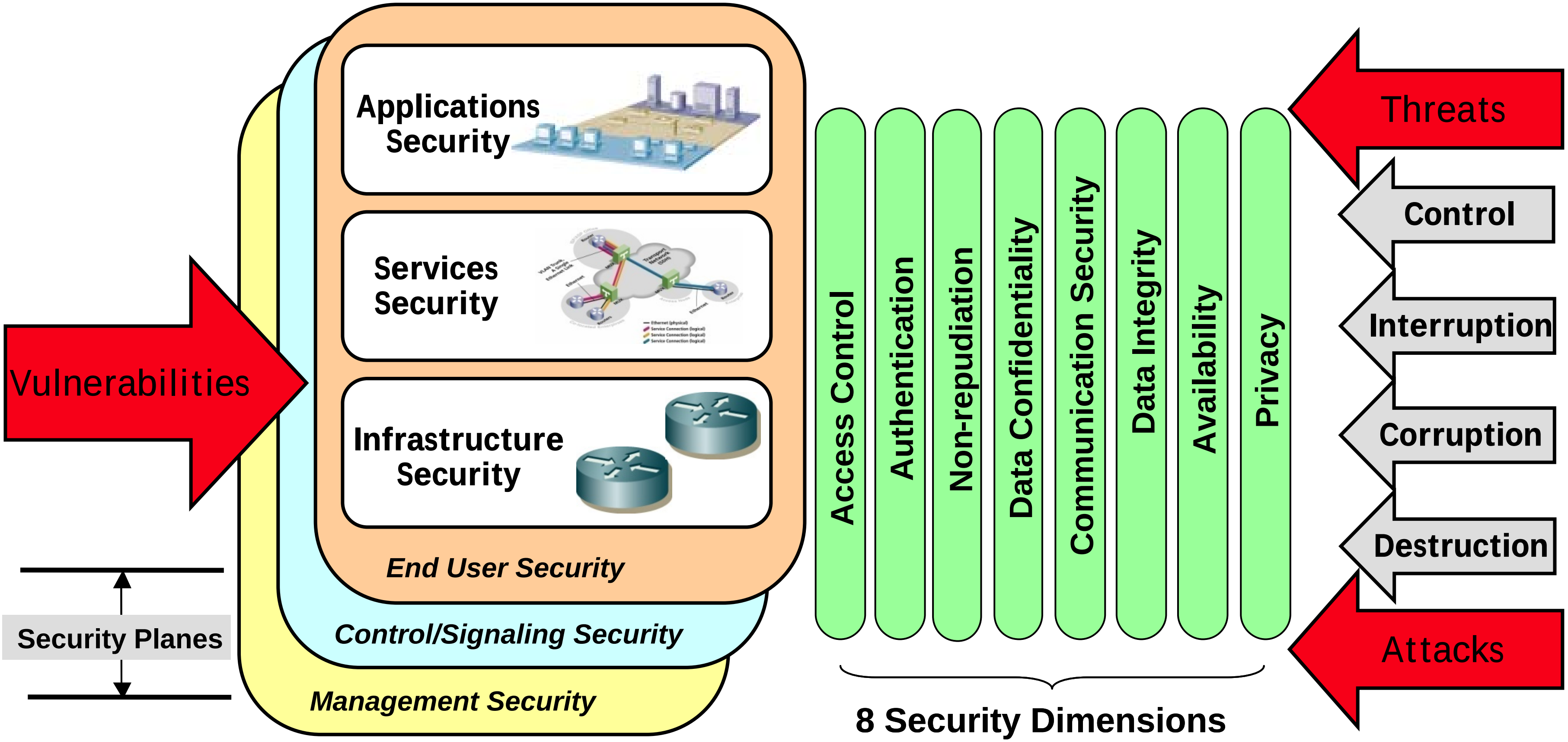
MAPPING SECURITY MANAGEMENT PROCESSES

ITU-T, TMFORUM, DoDAF CND OV-5



COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

SECURITY METHODOLOGY
APPLYING ITU-T X.805 SECURITY MODEL

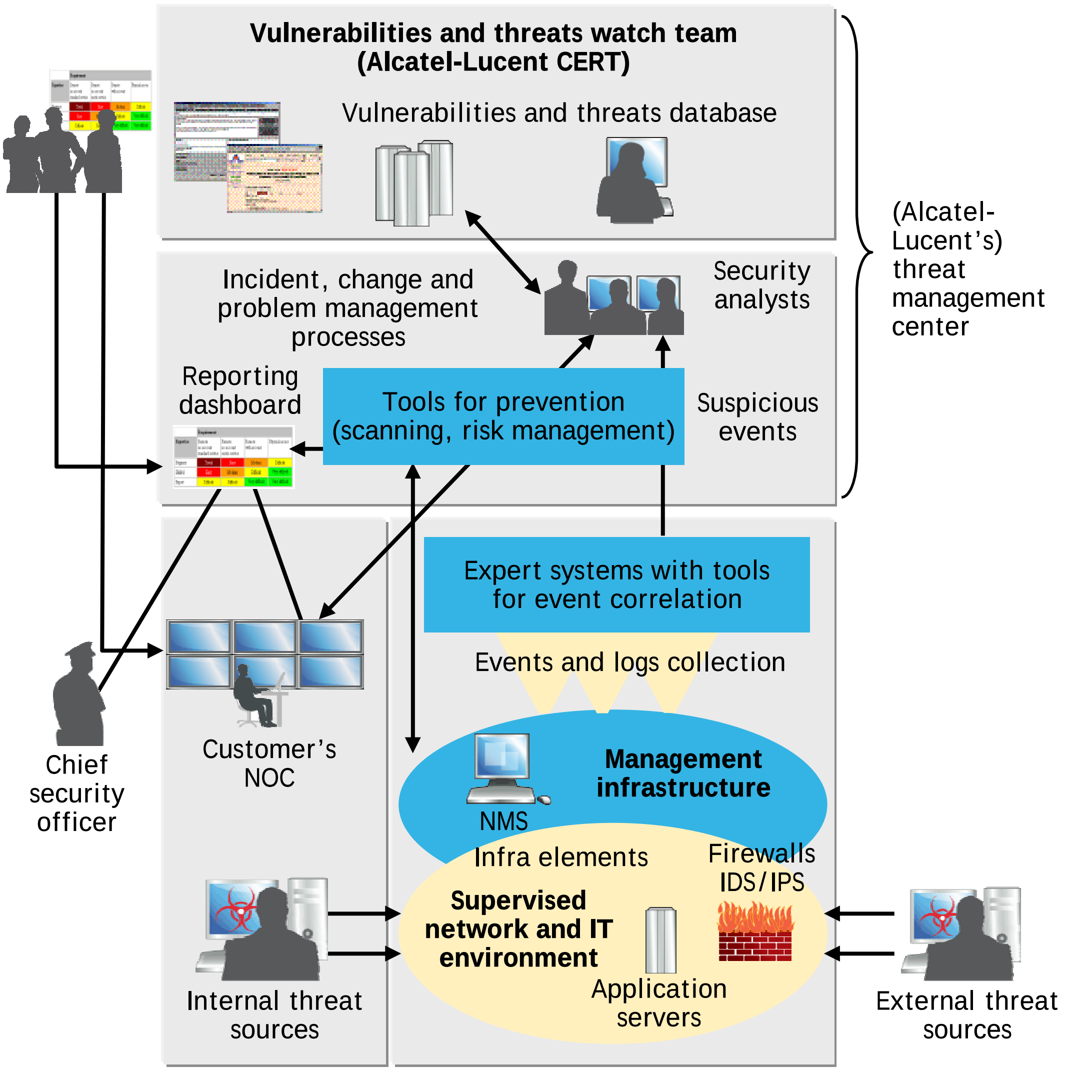


(Developed by Bell Labs)

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

SECURITY GOVERNANCE AND THREAT MANAGEMENT: HOW DOES IT WORK ?

- **Objective**
  - Provide ongoing advisory and monitoring services for customers who want to strengthen security controls and expertise, and simplify security operations and compliance reporting
- **What to do ?**
  - Security strategy, policy and compliance consulting
  - Vulnerability assessments
  - Attack simulation and service impact analysis
  - Threat and vulnerability advisories and alerts
  - Security event notification and customized reporting
  - Crisis management support



Vulnerabilities and threats watch team (Alcatel-Lucent CERT)

Vulnerabilities and threats database

Incident, change and problem management processes

Security analysts

Reporting dashboard

Tools for prevention (scanning, risk management)

Suspicious events

(Alcatel-Lucent's) threat management center

Expert systems with tools for event correlation

Events and logs collection

Chief security officer

Customer's NOC

Management infrastructure

NMS

Infra elements

Firewalls IDS/IPS

Supervised network and IT environment

Application servers

Internal threat sources

External threat sources

AT THE SPEED OF IDEAS

Alcatel·Lucent

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

THREAT MANAGEMENT & MANAGEMENT OF SECURITY Separation of duties

Customer

Network Operation Center

Security resource management

- Maintenance (fault management, monitoring,…)
- Patch management
- Deployment
- Change management
- Security rules configuration
- Operational incident management

ITIL-based processes
Incident mgmt
Change mgmt
Problem mgmt
Configuration mgmt

Threat Management Center

Security event monitoring

- Dashboard management & reporting
- Security Events and alarms management
- Security Policy compliance control
- Preventive Vulnerability Assess & Alerts
- Security Incident & crisis management
- Security in Change Advisory Board

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

CORRELATION BETWEEN SECURITY MECHANISMS & SECURITY FUNCTONS ENSURED IN A NETWORK INFRASTRUCTURE

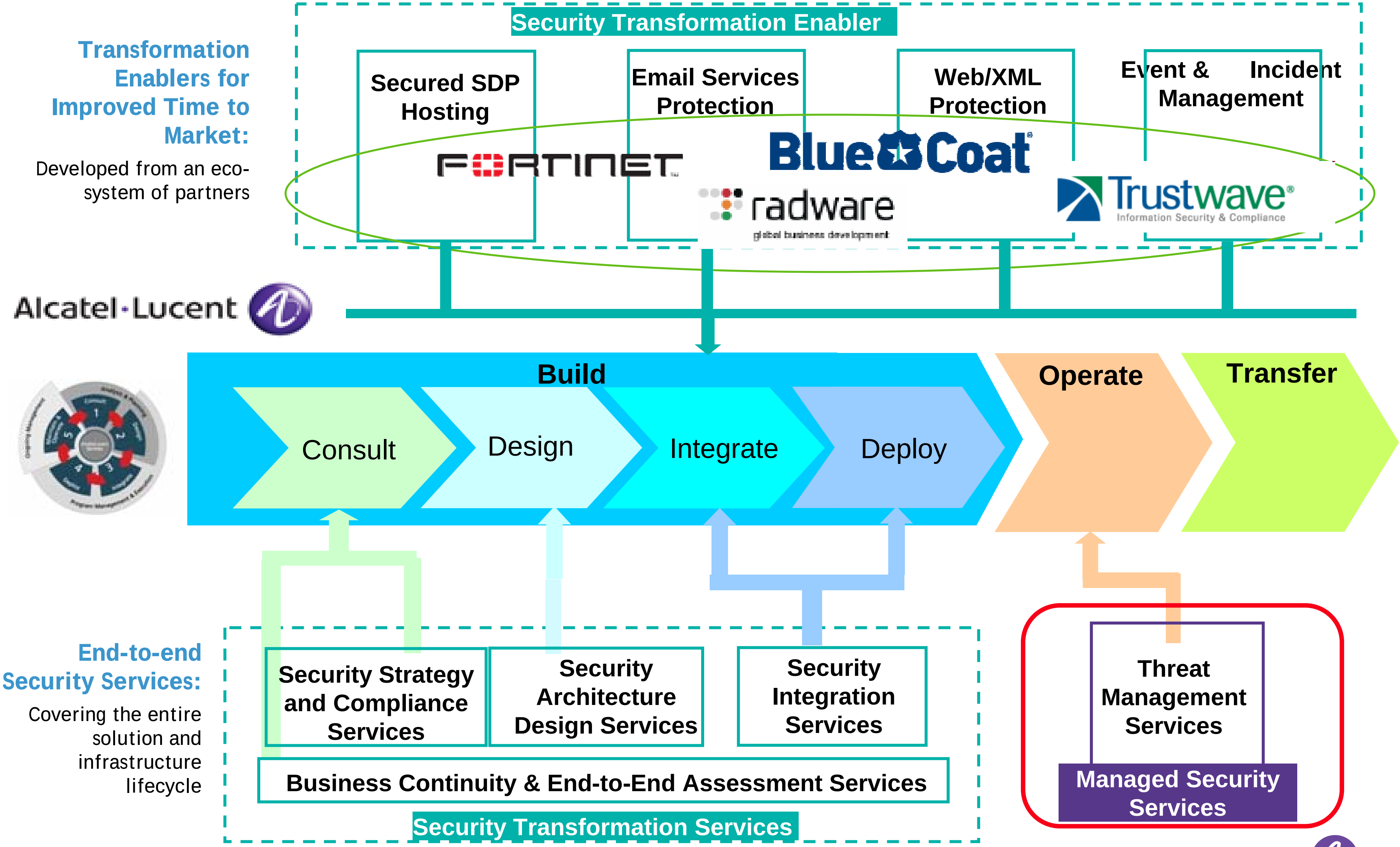
Service/ Mechanism	Encryption	Digital signature	ACL (Access Control Lists)	Data integrity	Authentication	Traffic padding	Routing control	Notorization	Recovery
Authentication	🟩	🟩			🟩				
Access control			🟩						
Confidentiality	🟩					🟩	🟩		
Data integrity	🟩	🟩		🟩					
Privacy	🟩						🟩		
Availability				🟩	🟩				🟩
Communication security							🟩		
Accountability		🟩		🟩				🟩	

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

SECURITY STANDARD OFFER

Main Services and Security Enablers

Applied to ALU solutions such as IMS, LTE, Cloud, OSS, BSS, 3G, 4G



Transformation Enablers for Improved Time to Market:

Developed from an eco-system of partners

Security Transformation Enabler

- Secured SDP Hosting
- Email Services Protection
- Web/XML Protection
- Event & Incident Management

End-to-end Security Services:

Covering the entire solution and infrastructure lifecycle

Security Transformation Services

- Security Strategy and Compliance Services
- Security Architecture Design Services
- Security Integration Services
- Business Continuity & End-to-End Assessment Services

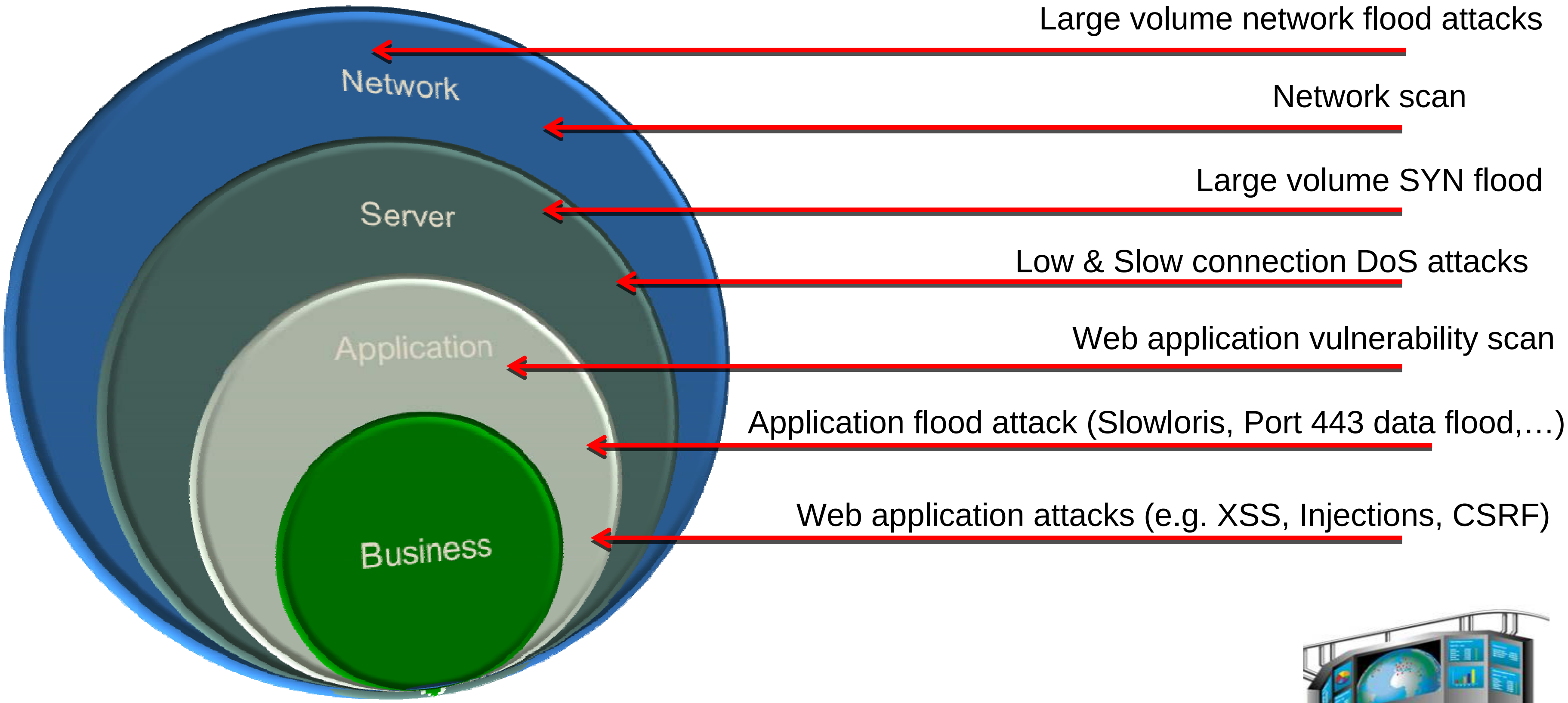
Managed Security Services

- Threat Management Services

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

DDOS MATTER ANALYSIS

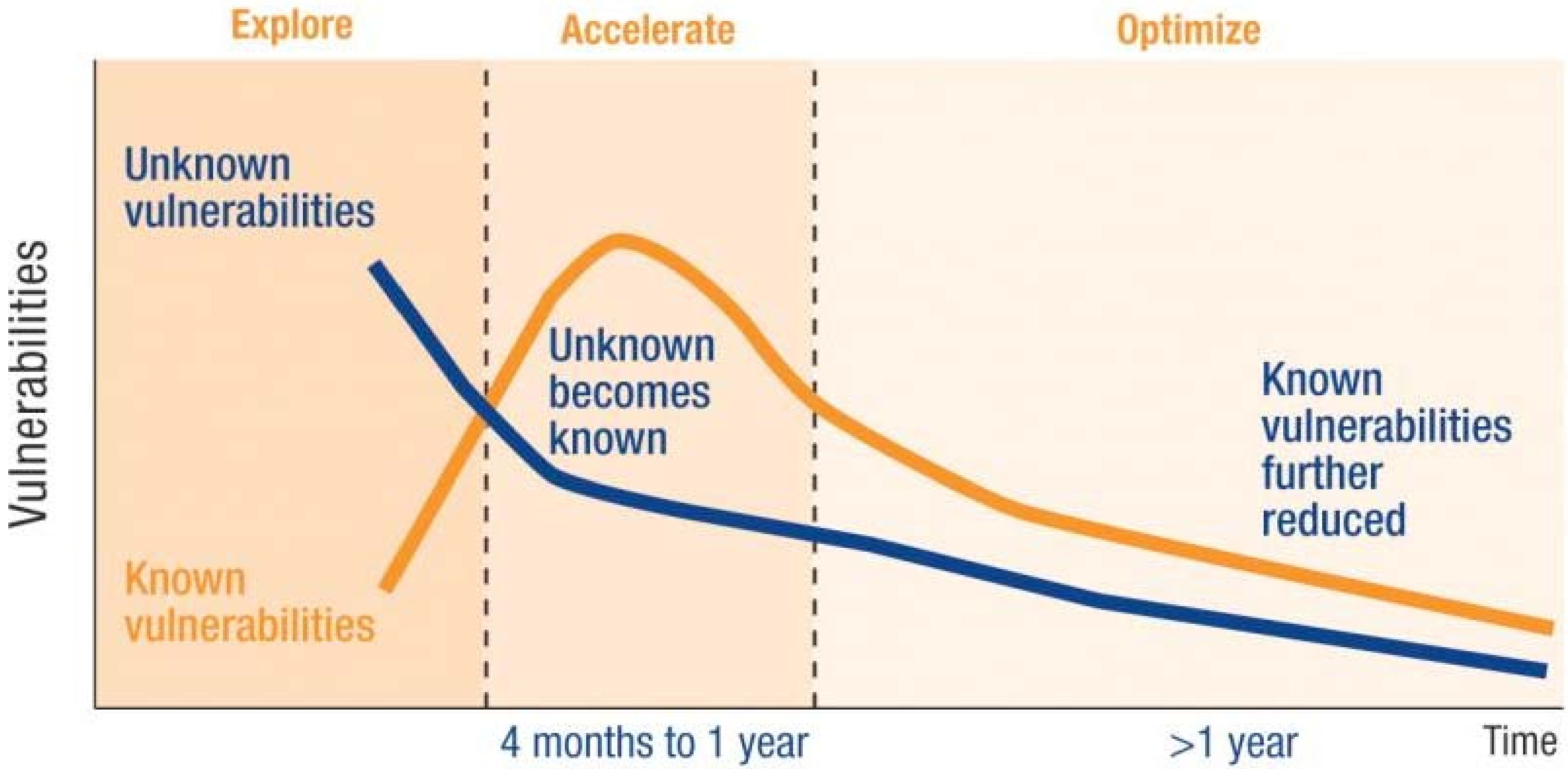
THE MULTI-VULNERABILY ATTACK CAMPAIGNS


Large volume network flood attacks
Network
Network scan
Server
Large volume SYN flood
Low & Slow connection DoS attacks
Application
Web application vulnerability scan
Application flood attack (Slowloris, Port 443 data flood,…)
Business
Web application attacks (e.g. XSS, Injections, CSRF)

Flexible approach, bundled & not following customers' requirements

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

EXAMPLE: SSA* CUSTOMER LIFECYCLE



Best practice companies were able to PREVENT vulnerabilities

Source: Mainstay Partners

*= Software Security Assurance

FORTIFY SOFTWARE

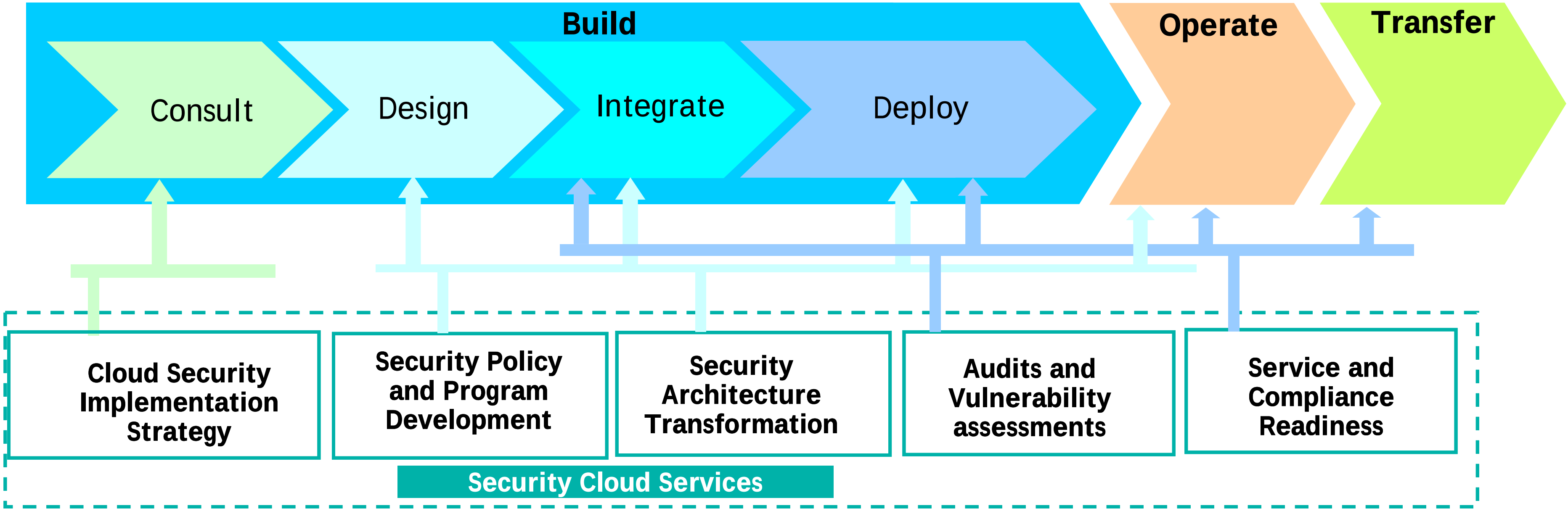
Alcatel·Lucent

AT THE SPEED OF IDEAS

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

CONSULTATION AND TRANSFORMATION SERVICES

An exhaustive set of assignments



Build
Operate
Transfer
Consult
Design
Integrate
Deploy
Cloud Security Implementation Strategy
Security Policy and Program Development
Security Architecture Transformation
Audits and Vulnerability assessments
Service and Compliance Readiness
Security Cloud Services

- *Customer Workshop*
- *Threat Assessment and Risk Analysis*
- *Security Architecture definition*
- *Service level definition*

- *Service Level Agreement Transformation*
- *Security Policy definition Support*

- *High Level and Detailed security designs*
- *Functional and non-functional requirements*
- *End-to-End Security Test Strategy*
- *Acceptance Plans*
- *Deployment specification*

- *Vulnerability assessment*
- *Penetration Testing*

- *Process review and readiness*
- *Security compliance and acceptance*

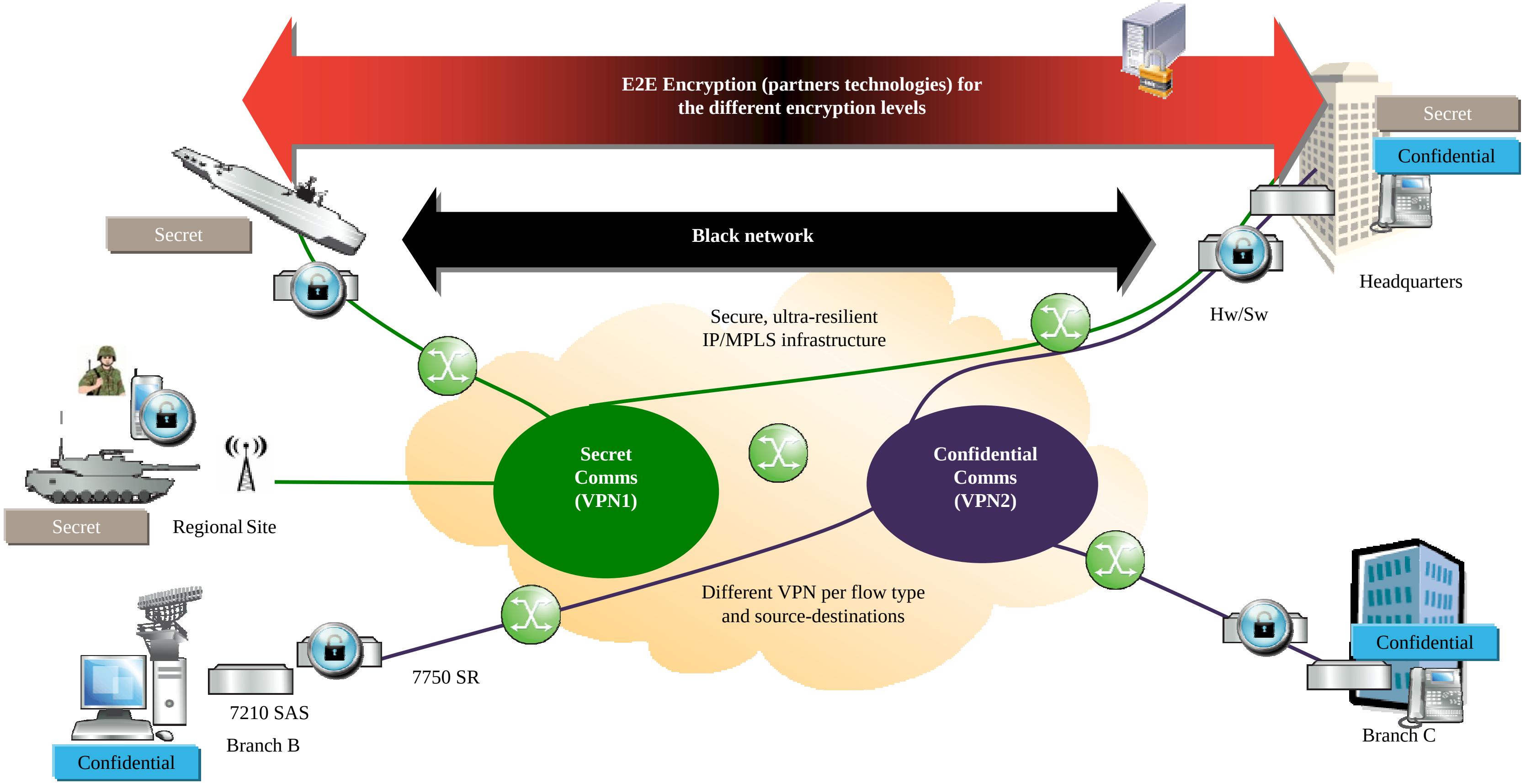
AT THE SPEED OF IDEAS

Alcatel·Lucent

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

SECURITY OPERATIONS MODEL FOR DEFENSE

Enforcing strong end-to-end encryption over a secure and resilient network infrastructure and separated fiber optic “to the user” for secret traffic

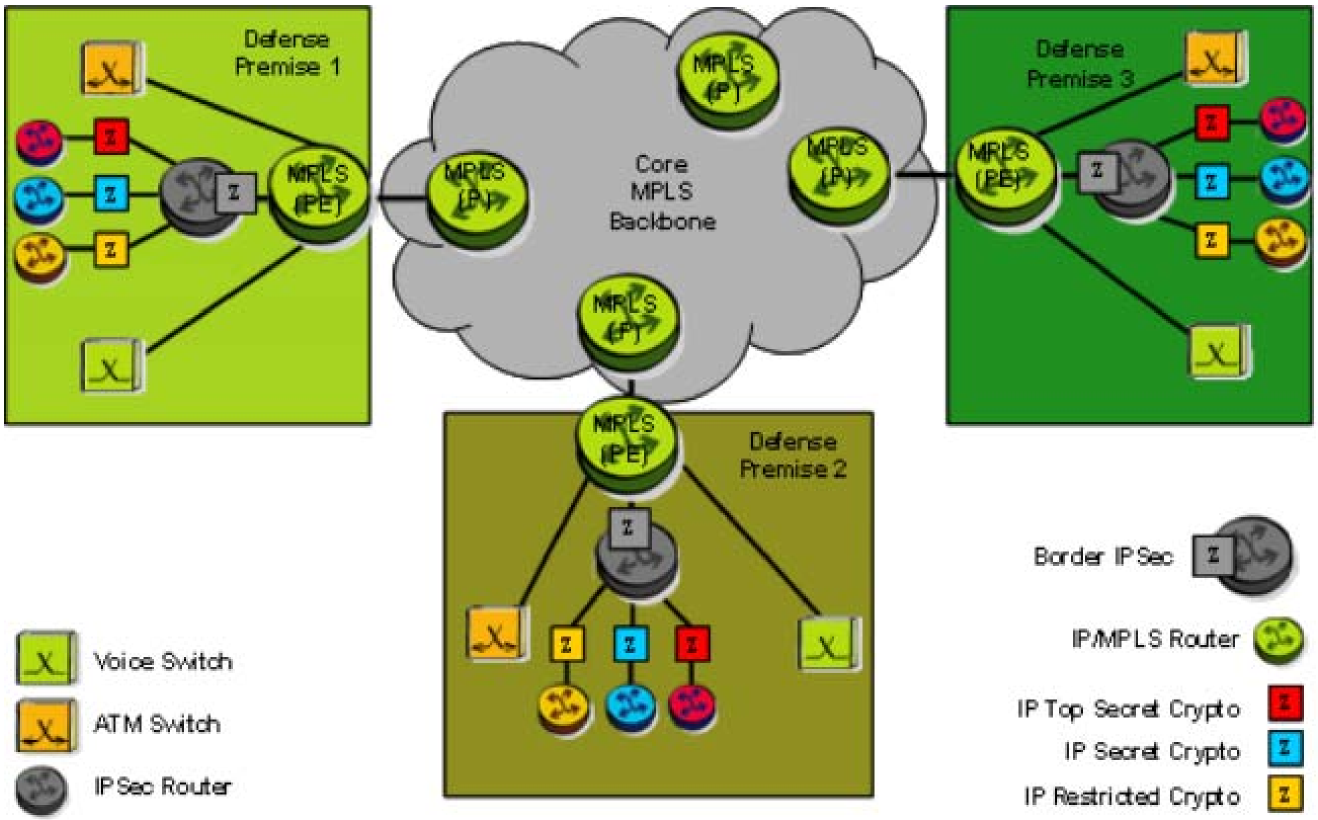


AT THE SPEED OF IDEAS

Alcatel·Lucent

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

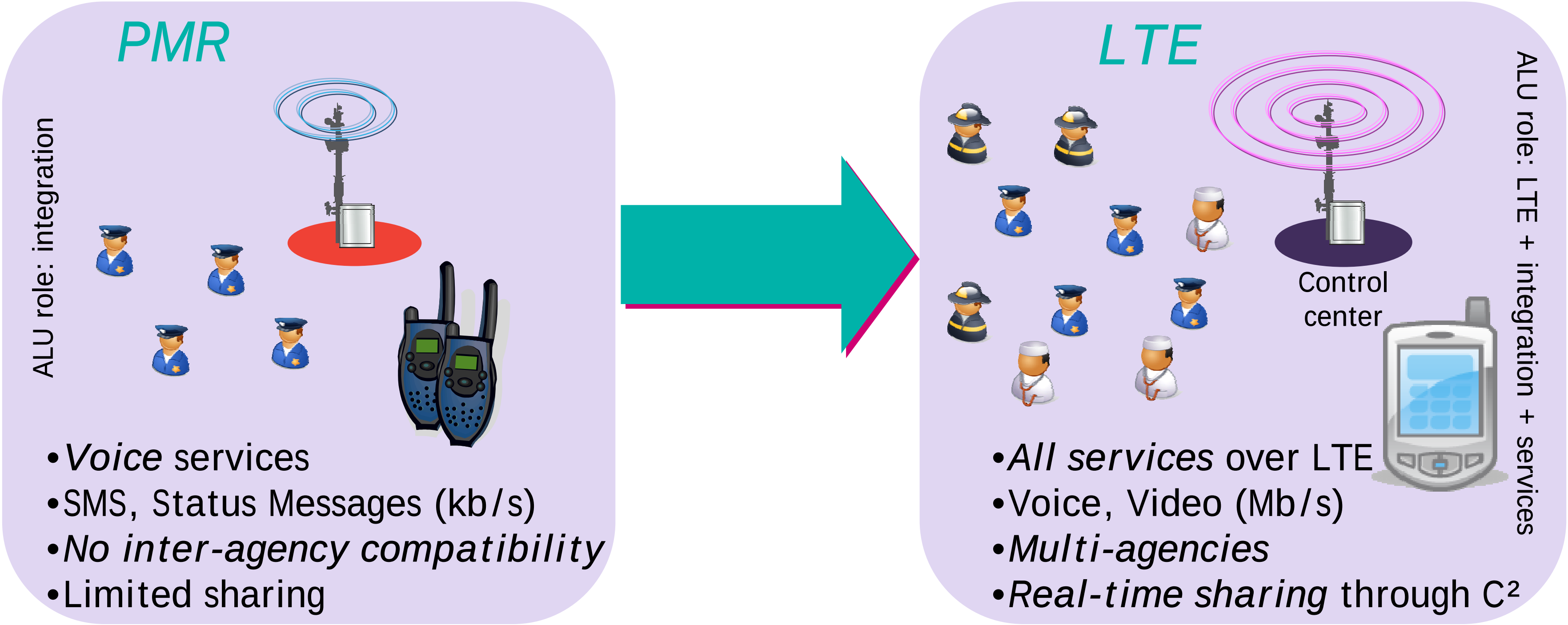
POSSIBLE MULTI-LEVEL SECURITY TARGET ARCHITECTURE FOR DEFENSE NETWORKS



AT THE SPEED OF IDEAS

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

FIRST RESPONDER OPERATIONS EVOLUTION



PMR

ALU role: integration

- *Voice* services
- SMS, Status Messages (kb/s)
- *No inter-agency compatibility*
- Limited sharing

LTE

Control center

ALU role: LTE + integration + services

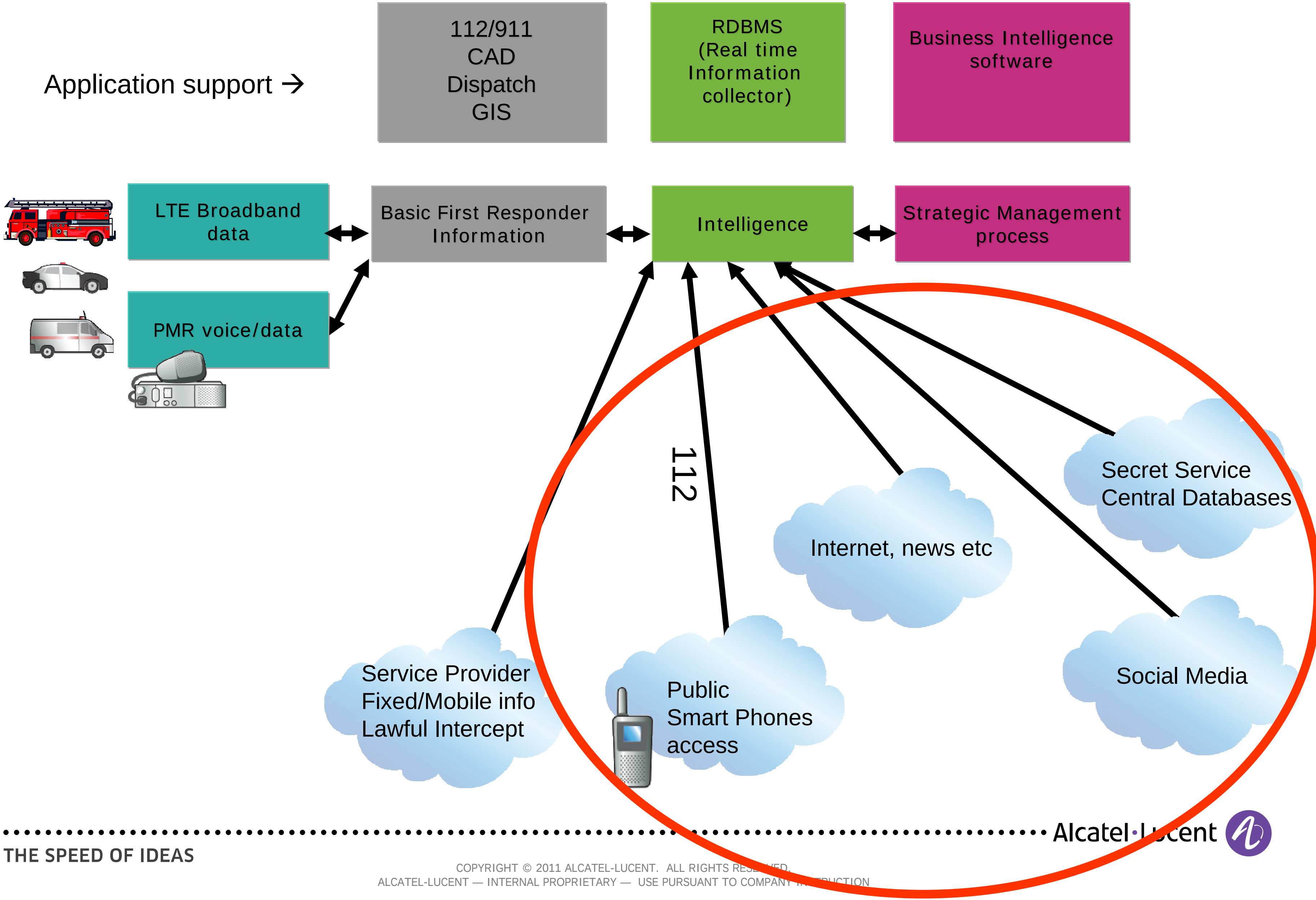
- *All services* over LTE
- Voice, Video (Mb/s)
- *Multi-agencies*
- *Real-time sharing* through C²

- ***Numerous added-value applications*** can be build on top of LTE with smart devices (mobile broadband inter-agency connection)
  - Real-time sharing of the situation, based on video, geo-localization, …
  - Augmented reality
  - Better coordination to speed-up support (location of support, blocked road, …)
  - Transfer of both (high-res) video, pictures combined with PMR voice for improved situational awareness

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

NEW DEVELOPMENTS

REAL TIME CRIME CENTER



Application support →

112/911
CAD
Dispatch
GIS

RDBMS
(Real time
Information
collector)

Business Intelligence software

LTE Broadband data

PMR voice/data

Basic First Responder Information

Intelligence

Strategic Management process

112

Service Provider
Fixed/Mobile info
Lawful Intercept

Public
Smart Phones
access

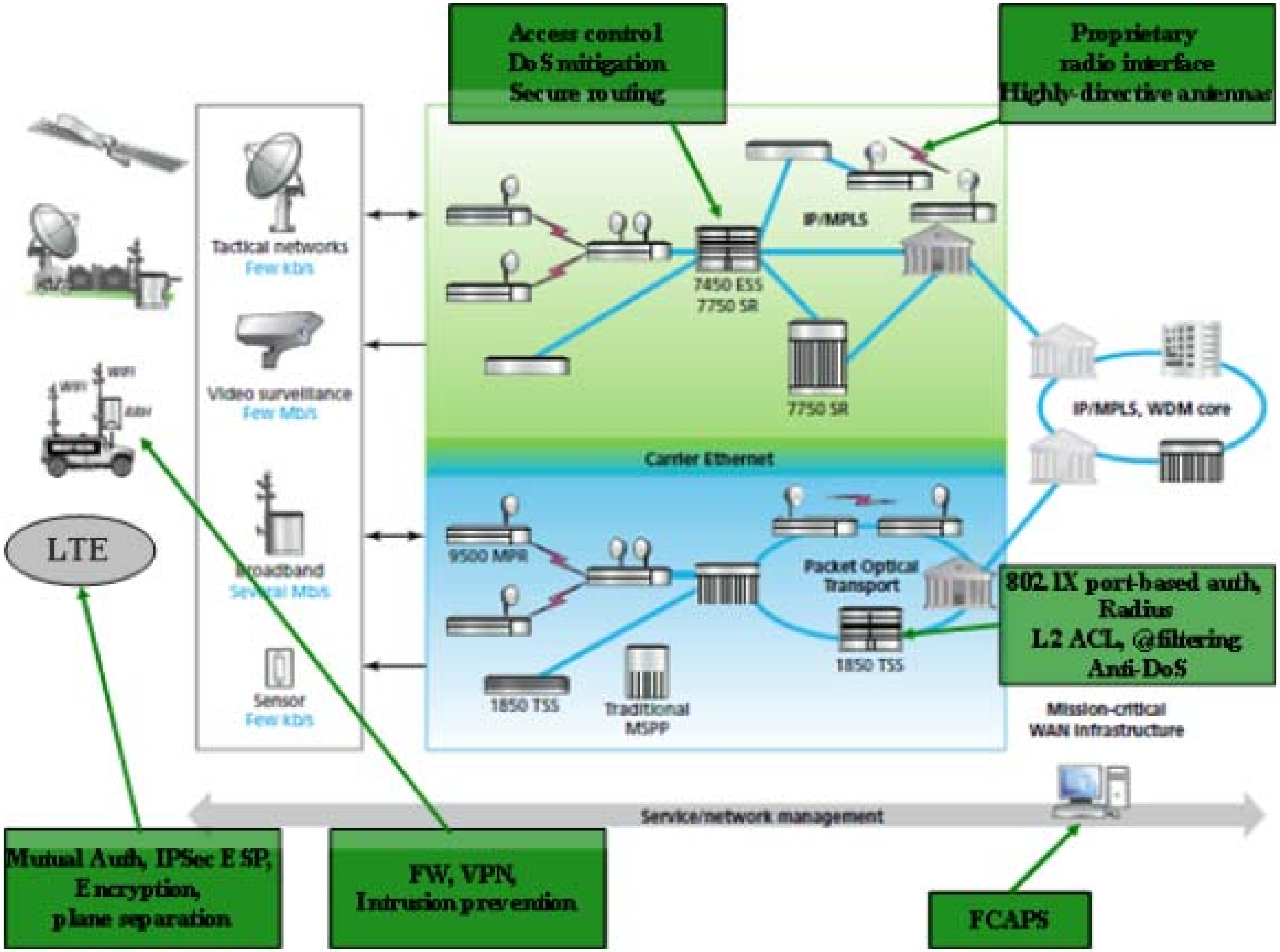
Internet, news etc

Secret Service
Central Databases

Social Media

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

SECURITY DISTRIBUTED OVER WAN & RAN FOR POLICE ORGANISATIONS



Access control
DoS mitigation
Secure routing

Proprietary
radio interface
Highly-directive antennae

802.1X port-based auth,
Radius
L2 ACL, @filtering
Anti-DoS

Mutual Auth, IPSec ESP,
Encryption,
plane separation

FW, VPN,
Intrusion prevention

FCAPS

AT THE SPEED OF IDEAS

Alcatel·Lucent

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

ALCATEL-LUCENT ADVISES THE EU COMMISSION ON ASSURING AVAILABILITY OF IT’s COMMUNICATIONS INFRASTRUCTURES

Analyzed the availability and robustness of communications infrastructures for the **European Commission**

Identified and **analyzed the impact of threats and vulnerabilities** on core (backbone), mobile and wireless networks. Developed recommendations for public authorities and industry players to mitigate risk and **secure Europe’s electronic communication infrastructures**. Final report and workshops involved participants from 27 EU member states as part of the European Commission’s Critical Infrastructure Protection Program.

EUROPEAN COMMISSION

What We Deliver

- Analysis of **vulnerabilities and threats** across critical **communication infrastructures**
- Collaborative **workshops** to **present key insights** and recommendations
- Documented findings from analysis, and **suggested approaches for mitigating risk** such as industry best practices, standardization, etc.

Value Proposition

- Identify vulnerabilities based on **knowledge of next-generation technologies** and experience designing highly available, robust networks
- Increase **awareness of reliability and security issues** across stakeholders

We have led the Cyber Tools On-line Search for Evidence research project for the European Commission, where our threat management services and CERT have been important differentiators in this domain.

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

ALCATEL-LUCENT DELIVERS IN-DEPTH SECURITY EXPERTISE FOR CNES

CENTRE NATIONAL D'ÉTUDES SPATIALES

- "Our relationship with Alcatel-Lucent allowed us to benefit from independent expertise for risk assessments and architecture design, as well as optimized computer incident response and crisis management."
- **Yvon Klein - Information Security Director, CNES**

Challenge

- CNES had key intelligence assets to protect and could not afford any disruptions in service within critical environments or locations, such as Kourou Launch pad.

Delivery

- Beginning in 1993, Alcatel-Lucent delivered more than 10 years of audit and risk assessment reports for CNES, and has secured more than 100 projects. Building a partnership with Alcatel allowed CNES to benefit from objective expertise and findings from audits and risk assessments. For crisis management, CNES co-founded (along with France Telecom) the CERT-IST, an internationally recognized watch, warn and alert center.

Benefits

- Independent expertise & specialized skills for audits, risk assessments and architecture design
- Mutual trust and long-term advisory relationship
- Strong escalation capabilities and crisis management support

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

ALCATEL-LUCENT HELPS U.S. Dept. OF ARMY IMPROVE THE SURVIVABILITY OF IT’s TELECOM INFRASTRUCTURE

Challenge

The U.S. Dept. of the Army has outlined a survivability plan for some of its major military facilities. An important component of this is the Total Switch Architecture (TSA), a master plan for implementation and evolution of voice services.

Delivery

Alcatel-Lucent provided a complete and comprehensive revision of the TSA for the Dept. of the Army, including a migration plan and recommendations for improved survivability. The results of the project were accepted by the customer without substantial change.

Benefits

- Alcatel-Lucent examined the entire public telecommunications infrastructure for major facilities with many thousands of office telephones.
- The project was completed on-time and the resulting consultancy report exceeded the expectations of the customer in both detail and completeness.
- The main benefit to the customer was the specification of a total switch architecture that improved survivability of telecommunications services, including reduced isolation of personnel and faster recovery to full service in the event of a disaster.
- Alcatel-Lucent was selected due to its long-standing successful track record in design and deployment of reliable and survivable telecom products and networks. Much of the existing implementation of the current TSA is based on Alcatel-Lucent products and this customer is satisfied with the performance.

The Department of the Army has determined that Lucent’s recommendations comprise the survivability model that it would like to implement for its voice communications system.

This customer reference was provided to Lucent Technologies prior to merger completion.

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

ALCATEL-LUCENT HELPS SERVICE PROVIDE CONSOLIDATE THE CORPORATE SECURITY PROGRAMM & PREPARE SAS 70 AUDIT

Challenge

A leading North American Service Provider needed to pass a SAS 70 audit in six months, while in the midst of migrating it services onto an IP/MPLS network and consolidating four separate security teams into a single corporate security unit. The Provider wanted to prepare for the audit with the eventual goal of becoming ISO compliant while developing an understanding of the return on investment (ROI) for its corporate security program initiatives.

Delivery

- Alcatel-Lucent Worldwide Services performed a pre-audit assessment that identified areas where control objectives and effectiveness needed to be addressed, and managed the progress of remediation activities completed for the audit. Alcatel-Lucent also developed a Security ROI model to predict and quantify the value of the corporate security program from both individual the business unit and security initiative perspective.

Benefits

- **Speed of completion.** Multiple projects were completed in ranges of weeks and months, with dedicated focus interviewing experts, reviewing documentation and analyzing data.
- **Third party objectivity.** Projects validated plans and provided necessary expertise for the serious challenges inherent in audit preparations and setting priorities for consolidation activities.
- **Helps Manage Uncertainty**. Security ROI model enables Provider to conduct sensitivity analyses on individual parameters to differentiate the benefits offered by individual corporate security initiatives. Additionally, Alcatel-Lucent experts are serving as trusted advisors throughout the actual audit process.
- **Continued Security.** As a direct result of these projects, the Provider accepted Alcatel-Lucent's recommendations and established a disciplined program management structure for its corporate-wide security program. Alcatel-Lucent is the Provider's partner for parallel projects involving its various networks.

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

CONCLUSION

- Cyber Security is a growing problem in years to come
  - **Greater complexity: Convergence, Web 2.0+, Virtualization, Cloud, Data privacy, Real time, without boundaries**
  - **Customers and governments beginning to realize this ...**
- Security is a growing factor in how customers view the quality and reliability of products, services, solutions
- Why Alcatel-Lucent ?
  - **Setting the standard & solving the network infra problem**
  - **Changing the landscape in partnership with customers & government**

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

CONCLUSION ?

"Information security is a major priority at this company. We've done a lot of stupid things we'd like to keep secret."

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

AT THE SPEED OF IDEAS

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION

THE 3-WAY HANDSHAKE OF CLOUD SECURITY

Understanding and responding all Challenges

3-Way
Security
Handshake

Transformation Planning Challenges

Understanding each situation and proposing adequate measures

Customer Compliance requirements, Impacts on the Provider/Customer Security Policy and SLAs, Data Classification model, SLAs for Security monitoring, reporting…

Technical and Virtualization Challenges

Traditional and Specific Cloud Security solutions

Virtual Firewall, IDS/IPS, Logging and reporting, Change Control Management and Compliance monitoring, Vulnerability scanning, Database Security…

Operational Challenges

What level of services for the Cloud provider and for the customers

Log retention, Incident Management, Change Control &Patch Management, Security Provisioning, Identity and Access Control, Compliance and Vulnerability Monitoring…

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
ALCATEL-LUCENT — INTERNAL PROPRIETARY — USE PURSUANT TO COMPANY INSTRUCTION