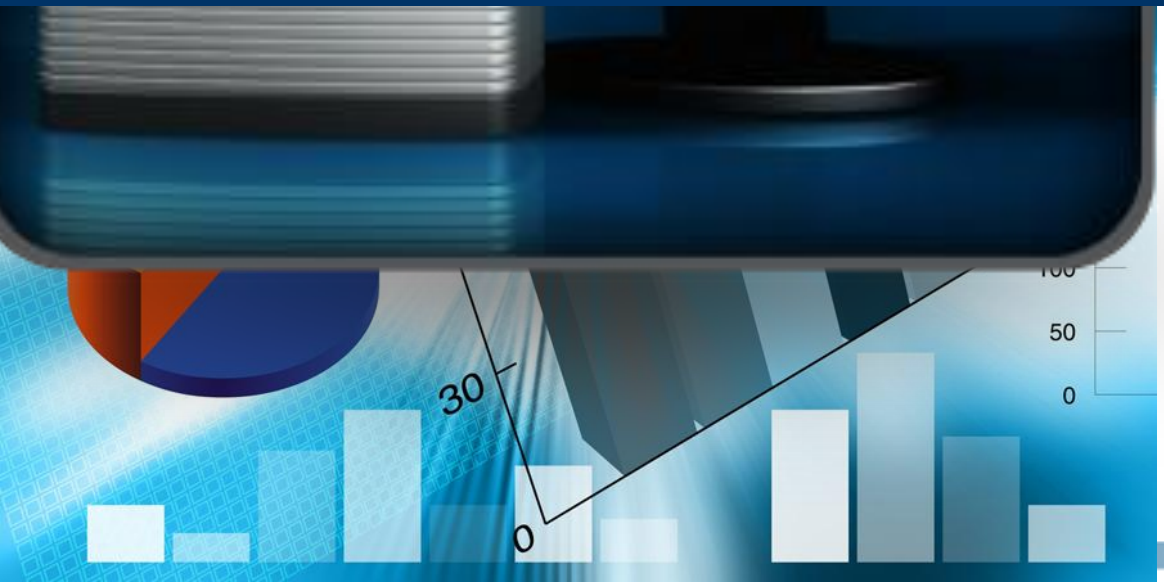
Economic Tides, Technology Trends & Security Threats



Walter Lee
CEO
e-Cop Group

e-Cop®
Managing Risk. Securing Enterprise.

Agenda

- e-Cop in the Asia Pacific Region
- Tides, Trends and Threats:
  - ✓ Cloud Computing
  - ✓ Mobility Wave
  - ✓ Social Networks
  - ✓ Internet TVs
- Q & A

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Company Profile

- E-COP.NET: Network for Electronic Crimes and Online Protection
- Subsidiary of Certis Cisco Security
- Established in 2000
- Plays a leadership role in shaping the info-security landscape
- Pure-Play Managed Security Services Provider (MSSP)
- Group staff strength > 160

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Company Profile

- Headquartered in Singapore with offices in Malaysia, Hong Kong, Thailand, and India
- Presence in more than 20 countries in the region through partners
- Security Operation Centres (SOCs) powered by award-winning Cyclops Enterprise Security Manager
- Operating the largest network of ISO/IEC27001 certified SOCs in the region

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Our Expertise

e-Cop
Managing Risk. Securing Enterprise.

Managed Security Services

Manage, Monitor, and Respond

- Outsource Security Monitoring
- Compliance Monitoring
- Network IDS Subscription + Monitoring
- Outsource Log Analysis
- Outsource Security Device Management

Professional Security Services

Assess and Audit

- ISO 27001 / BS 7799 / Risk Management
- Penetration Testing & Vulnerability Assessment
- Network Security Reviews & Forensics
- Systems & Process Audits
- ICT Security Framework
- CERT / CSIRT
- Security Health Scorecard

Technology Consulting Services

Design and Deploy

- Security Management
- Security Event Analysis
- Information Management
- Endpoint Security
- Information Integrity
- Network IDS
- Security Architecture

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Expansion Updates

❖ Regional Joint-Ventures

- ✓ Thailand JV – Bay Computing (November 2010)
- ✓ India JV – Allied Digital System (April 2011)

❖ Acquisition

- ✓ Vectra Information Security Pte Ltd (VIS)
- ✓ August 2011 (100% Ownership)

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Acquisition of VIS

- **Vectra Information Security Pte Ltd**
- **Background**
  - ✓ **Wholly Owned Subsidiary of e-Cop Pte Ltd**
  - ✓ **Leading Security Consulting Firm in Asia Pacific**
  - ✓ **Appointed Qualified Security Assessor (QSA) by Payment Card Industry (PCI) Security Council since 2009**
- **Services**
  - ✓ **PCI Data Security Standard Compliance Services**
    - **Consultancy and Assessment**
    - **Validation Services**
  - ✓ **Security Risk Assessment Services**
  - ✓ **IT Security Review**

VECTRA CORPORATION

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Our Footprints

Copyright 2000-2009 e-Cop. All rights reserved worldwide.

e-Cop Global Command Centre

- **Intelligence feeds obtained from:**

FIRST Forum of Incident Response and Security Teams

GCC's Intelligence Knowledge Base

Our Security Partners

- Solutionary
- McAfee
- Trend Micro
- Sourcefire

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Trust Indicators

3.0 Billion
Events Processed in 2010

Widest
Network of ISO/IEC27001 Certified SOCs in the Region

Largest
Customer Base in the Region

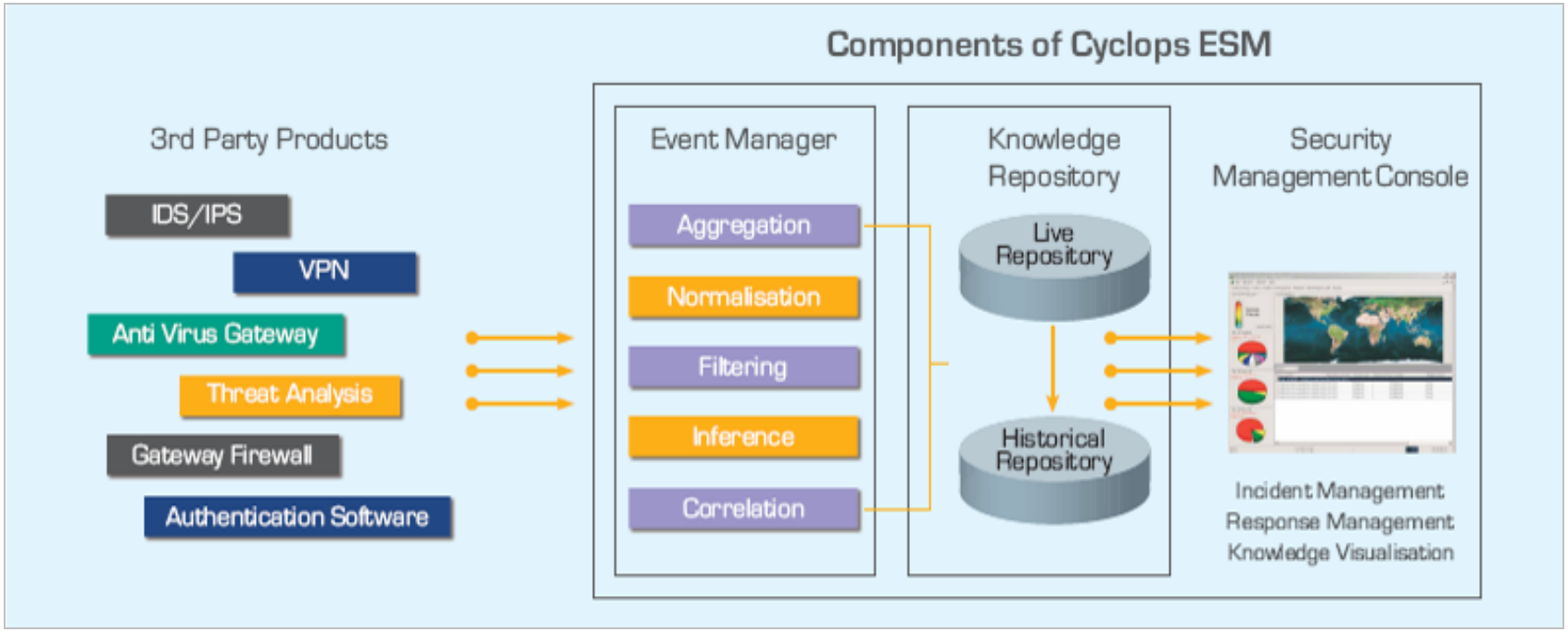
Over 1,600
e-Gov't Applications Secured

The Most
Number of Logs Managed and Analysed

Pioneering
Cyber Security Intelligence in the Region

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Cyclops Security Solutions



Proactive, flexible, and non-intrusive enterprise security management system

Provide insights into security incidents before, during, and after they occur

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

At-A-Glance

PEOPLE

Fully qualified Security Consultants
CISSP
CISA
CISM
BS7799/ISO27001 Lead Auditor

PROCESS

Based on world standard BS7799/ISO27001

1st BS7799/ISO27001 certified Info-Security service provider

Audited by BS7799/ISO27001 auditor every half a year

TECHNOLOGY

Vendor independent and non-intrusive technology

Award-winning technology

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Research & Development

- **Up to 10 % Revenue Investment into R&D**

- **CESM System powered by CIESEH – for evaluation under Common Criteria (CC) or ISO15408 under Evaluation Assurance Level (EAL) 4.**

  "…No other SIEM has achieved as of today"

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Technology Patents

- **4 Registered Patents**
  - US2004/0250133A1-09122004 — **Computer Security Event Management System**
  - US2005/0187987A1-25082005 — **Managing Transaction Log Data**
  - US2006/0026683A1-02022006 — **Intrusion Protection System And Method**
  - US2007/0289013A1-13122007 — **Method and System for Anomaly Detection using a Collective set of Unsupervised Machine-Learning Algorithms**
- **10 Provisional patents status granted in Singapore, Malaysia, Brunei & US**
- **30+ Potential target patents**

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Significant Milestones

e-Cop
Managing Risk. Securing Enterprise.

FIRST
Improving Security Together
Forum of Incident Response and Security Teams

e-Cop , member of FIRST

CORPORATE EXECUTIVE PROGRAMME

e-Cop, inaugural member of CEP

Common Criteria

Common Criteria
e-Cop embarked on EAL4

Microsoft Partner
Silver Independent Software Vendor (ISV)

Microsoft Silver Certified Partner

Independent Software Vendor (ISV)

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Key Achievements

Information Security Service Provider of the Year 2009

Winner for Security - Cyclops ESM
Merit for e-Government - CWC

F&S MSSP Of The Year
2005 2008 2009 2010

CIO 100 Honouree 2005 & 2007

Info-Security Product Guide - Security Hot Company 2007

2006 & 2007 China Information Security - Most Trusted Brand Award

Most Innovative Product/Service
National Infocomm Award 2004

Rated "Positive" for MarketScope for MSSP in Asia Pacific 2010

Computerworld Editor's Choice
for 2003 Catalyst Award

Only recipient for 24x7 Info-security monitoring

Cyclops IDS

Copyright © West Coast Publishing

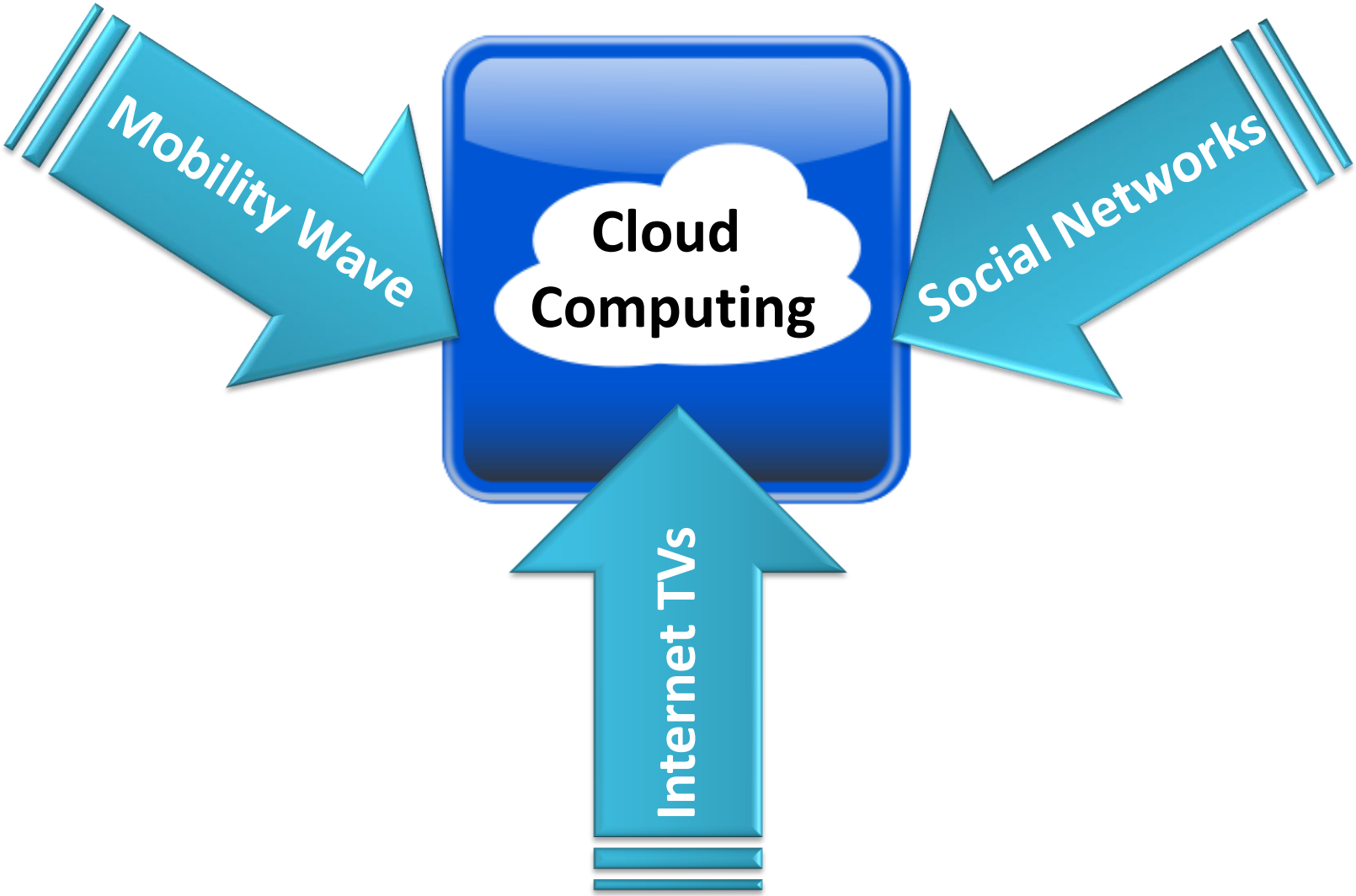
Endorse By

e-Cop's National e-Security Defence Strategy

ISO 27001 Certified

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Cloud Computing



Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Types of Cloud Service Models

1) Platform as a Service (PaaS)

Allows users to run existing applications or develop new ones by providing them with virtualized servers

2) Infrastructure as a Service (IaaS)

Allows users to deploy & run arbitrary software by providing them with processing, storage, networks & other computing resources

3) Software as a Service (SaaS)

Allows users to use the provider's applications which are run on a cloud infrastructure

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Cloud Deployment Models

Public Cloud

- ✓ Infrastructure is available to the general public or a large industry group
- ✓ Owned by the cloud service provider

Private Cloud

- ✓ Infrastructure is available only to a organisation
- ✓ Managed by the organisation or 3rd party
- ✓ May exist on-site or off-site

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Cloud Deployment Models

Community Cloud

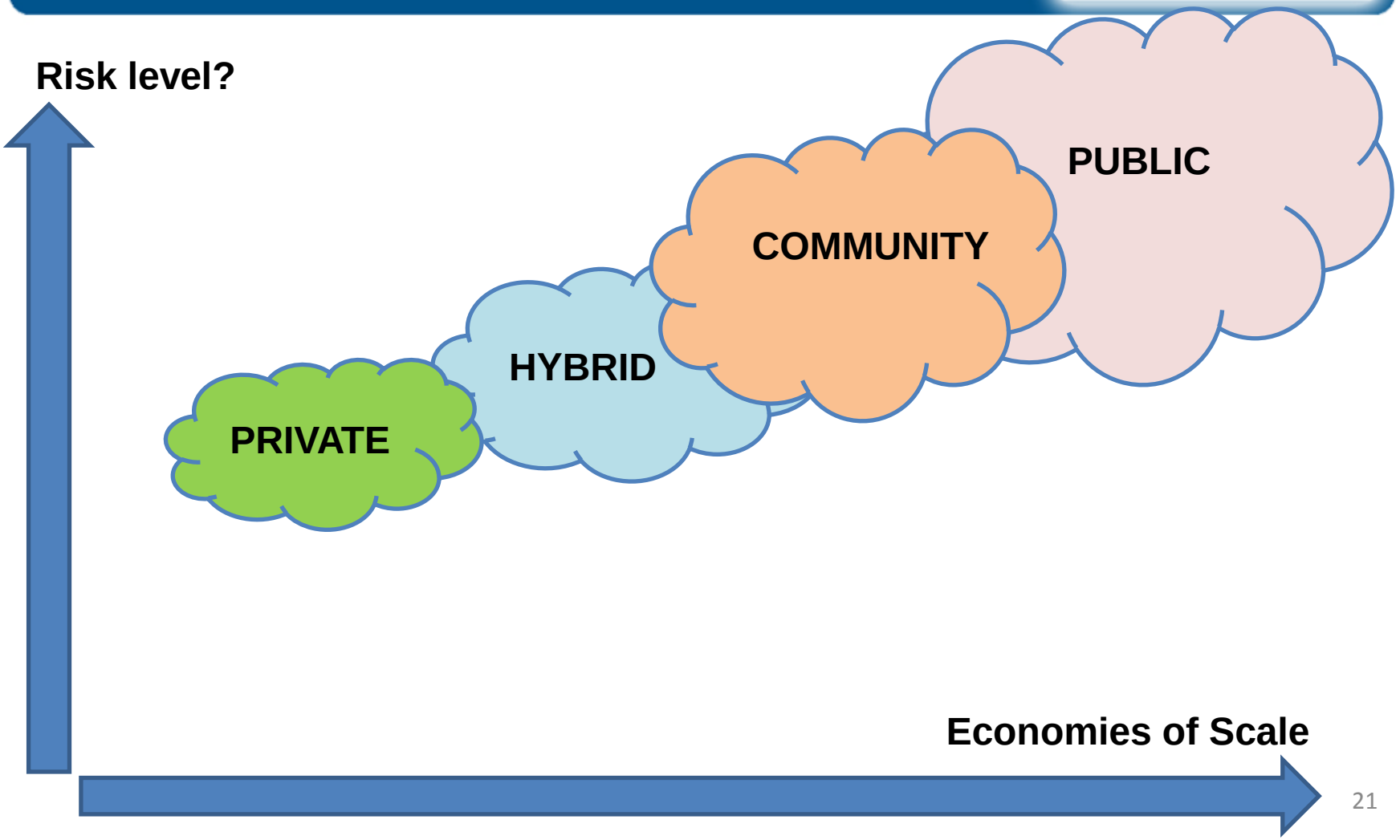
- ✓ Infrastructure is shared by several organisations & supports a specific community with shared concerns
- ✓ Managed by the organisations or a 3rd party
- ✓ May exist on-site or off-site

Hybrid Cloud

- ✓ Infrastructure is comprised of 2 or more clouds (private, community or public)
- ✓ Remain as unique entities but are brought together by a standardised or proprietary technology
- ✓ Enable a balancing of workload between clouds

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Risk levels?



Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Cloud Computing

Source: CIO , 6 September 2011

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Cloud Computing

e-Cop
Managing Risk. Securing Enterprise.

Asian Market

- ✓ Market for cloud computing is expected to reach **$3.2 billion this year**, a **71% growth** from $1.87 billion last year (Source: Reuters Taipei, 3 June 2011)
- ✓

Global Market

- ✓ Could reach **$55 billion in 2014**

  (Source: Reuters Taipei, 3 June 2011)

Photo: Cloud Computing Techie

BUT concerns over security could slow down the market growth

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Security Concerns on Cloud Computing

Hacker attacks threaten to dampen cloud computing's prospects

Recommend 44 people recommend this.

Tweet 199

Share 110

Share this

Email

Print

Related News

U.S. weighs se after "serious" Google allegati
Thu, Jun 2 2011

Microsoft show Windows 8 ope system
Thu, Jun 2 2011

Google reveals hacking, says I from China

By Clare Jim and Lee Chyen Yee

TAIPEI | Fri Jun 3, 2011 5:42am EDT

(Reuters) - The recent high-profile hacking of Google's Gmail service and Sony's Playstation gaming network is threatening to slow the take-off of the next big thing in the computing space - the cloud.

Source: Reuters (Taipei) , 3 June 2011

"Many enterprises have **reservations about the security of cloud computing** because of the multi-tenant architecture and the fact that cloud providers are 'big targets' "

Steve Hodgkinson, IT research director at UK-based research firm Ovum
3 June 2011

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Security Concerns on Cloud Computing

- Vulnerability to cyber attacks
- Disruptions to data center operations
- Exposure of confidential/sensitive information to unauthorized systems or personnel
- Inability to support forensic investigations
- Inability to support compliance audits
- Loss or leakage of confidential/sensitive data
- Weak access control over system and/or application
- Legal implications arising from breach of contract

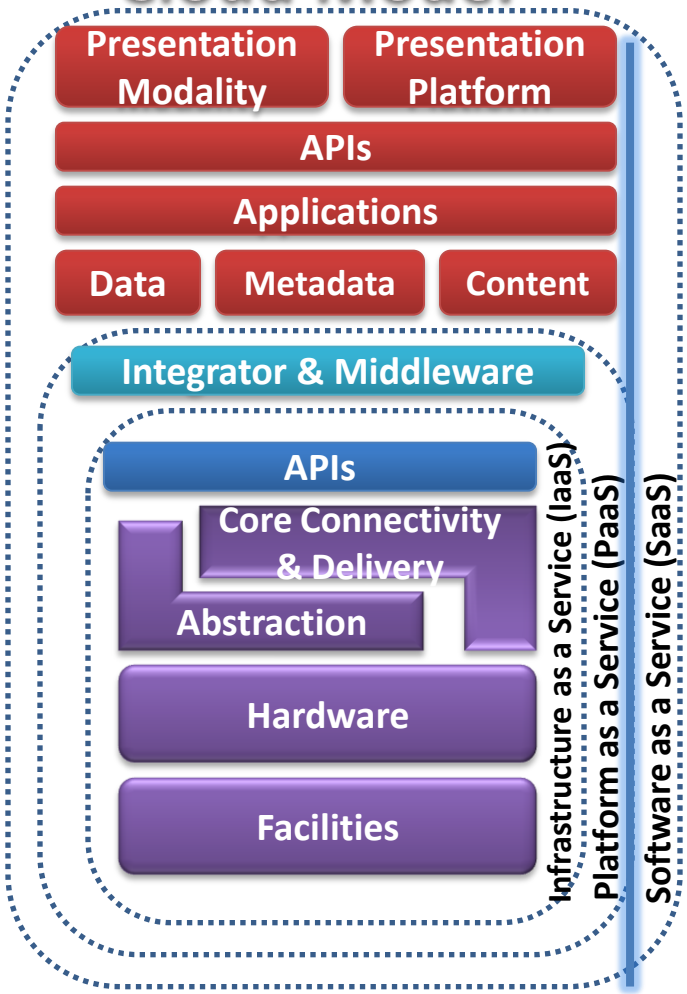
Photo: ACM News

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Mapping Security Control & Compliance to the Cloud Model

e-Cop
Managing Risk. Securing Enterprise.

Cloud Model



Source: Cloud Security Alliance

Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/ IDS/ IPS
- ☑ Patch/ Vulnerability Management
- ☑ Physical Access Control
- ☑ Two-Factor Authentication…

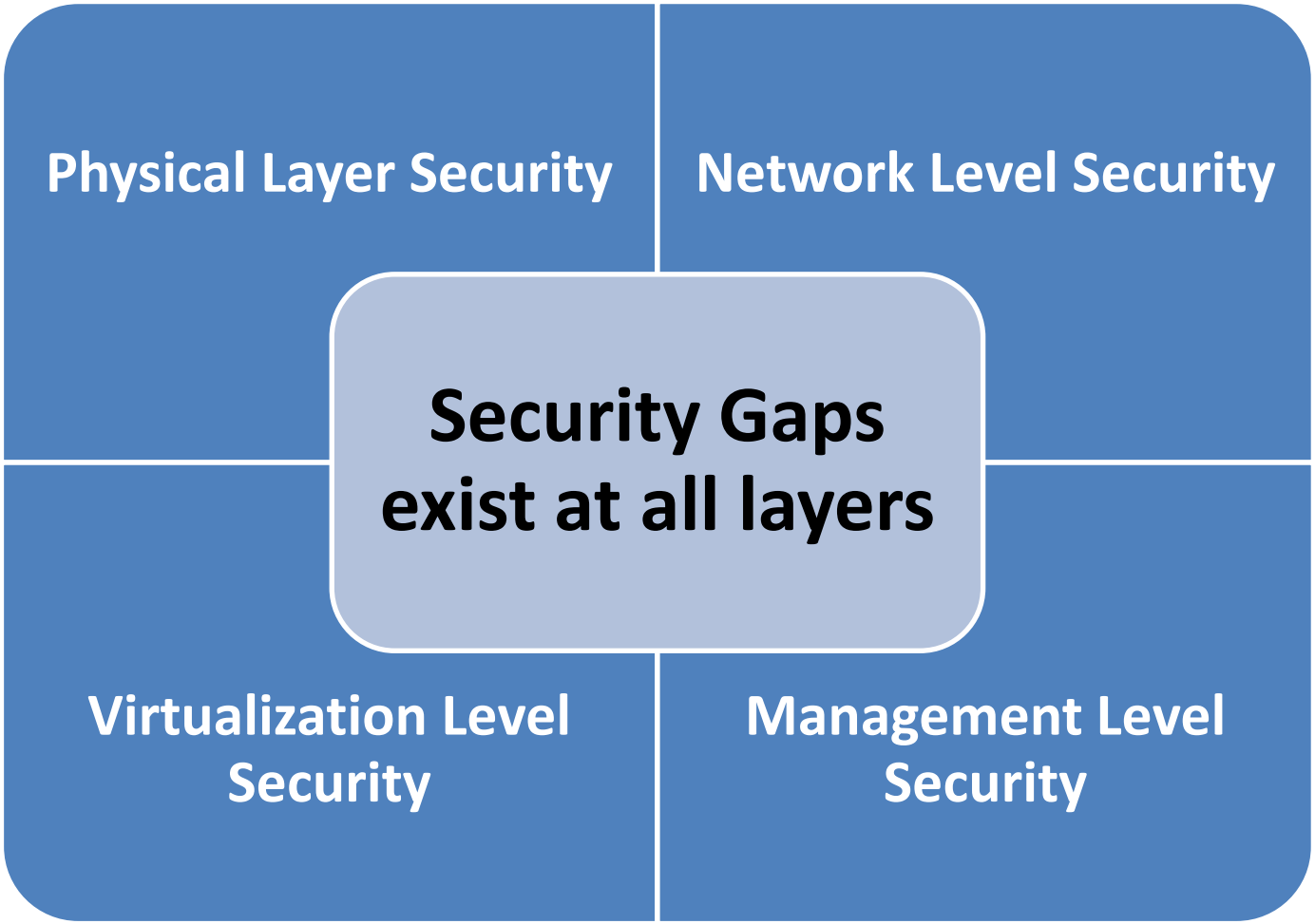
HIPAA

GLBA

SOX

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Security Concerns on Cloud Computing



Copyright 2000-2011 e-Cop. All rights reserved worldwide.

e-Cop can help to perform "Check and Balance"

- **Intrusion Monitoring** to **protect** the cloud from cyber attacks such as DDOS

- **Compliance Monitoring** to ensure that the cloud provider **maintains** its policy guidelines

  e.g. PCI monitoring of cloud providers that transact internet payments

- **Independent System Audit** to ensure that cloud providers are able to **comply** to policy

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Mobility Wave

- Proliferation of mobile technologies
- Increasing usage of smartphones, tablets and laptops in the business world
- Employees can take the enterprise anywhere!
- **1.2 billion mobile workers worldwide by 2012**

(Source: TODAY online, 19 September 2011)

Photo: Liberty Mobiles

Photo: Tablets.com

Photo: TFTS

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Mobility Wave

- Recent Global IDC Survey: **69%** of respondents worldwide **use a smartphone for business purposes**

Source: IDC, 12 September 2011

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Security Concerns on Mobility Wave

Source: CIO, 6 September 2011

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Security Concerns on Mobility Wave

AT RISK: GLOBAL MOBILE THREAT STUDY FINDS SECURITY VULNERABILITIES AT ALL TIME HIGHS FOR MOBILE DEVICES

400 Percent Increase in Android Malware Found Since Summer 2010

SUNNYVALE, Calif., May 10, 2011 — In a global mobile threat study released today, Juniper Networks (NYSE: JNPR) found that enterprise and consumer mobile devices are exposed to a record number of security threats, including a 400 percent increase in Android malware, as well as highly targeted Wi-Fi attacks. Through close examination of recent malware exploits, the study outlines new areas of concern and delivers clear recommendations on essential security technologies and practices to help consumers, enterprises/SMBs, and government entities guard against mobile device exploits.

With smartphones set to eclipse PCs as the preferred method of both personal and professional computing, cyber criminals have turned their attention to mobile devices. At the same time, the gap between hacker capabilities and an organization's defenses is widening. These trends underscore the need for further mobile security awareness, as well as more stringent, better integrated mobile security policies and solutions.

Source: Juniper Networks, 10 May 2011

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Security Concerns on Mobility Wave

TECHNEWSWORLD
ALL TECH - ALL THE TIME

Microsoft
DON'T GET FORCED. GET W
Switch and get $150/user

NETWORK INTRUSION

Computing | Internet | IT Management | Mobile Tech | Security | Technology

TechNewsWorld > Security > Network Intrusion | Read Next Article in Network Intrusion

EXPERT ADVICE

It's Cold Out There: Protecting Data Outside the Enterprise Firewall

Print Version
E-Mail Article
Reprints

By Rob Marano
TechNewsWorld
05/02/11 6:00 AM PT

The advancement of mobile technologies has enabled employees to take the enterprise anywhere -- both at home and on the road. But with a greater amount of work being done outside the firewall, criminals have begun to target their attacks accordingly. Companies must incorporate security policies and mechanisms that define and automate how sensitive information should be handled at the file level.

Source: TechNewsWorld, 05 February 2011

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Security Concerns on Mobility Wave

- Data leakage as a result of lost or stolen devices
- Risks arising from sending of confidential documents through unsecured networks
- Gaps in device management & policy enforcement
- Exposure to new cyber-vulnerabilities relating to private data and Intellectual Property (IP)

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

e-Cop's Role

Secure Network Architecture Assessment Service

- ✓ Existing firewall infrastructure
- ✓ Routers
- ✓ Exposed services
- ✓ External network links
- ✓ Virtual private networks
- ✓ Remote access services

Systems & Process Audit Services

- ✓ Audit security policies, procedures & systems
- ✓ Pinpoint gaps & recommend security policies that define how sensitive information should be handled

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Vietnam: Internet Access

- Recent launch of a project on "Improvement of computer usage and public internet access in Vietnam" by Vietnam's Ministry of Information and Communications (MIC)

- Projected to reach around 760,000 new users spanning 40 provinces

- Will expand access to e-government services at the local level amongst other benefits

(Source: Bill & Melinda Gates Foundation, 10 November 2011)

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

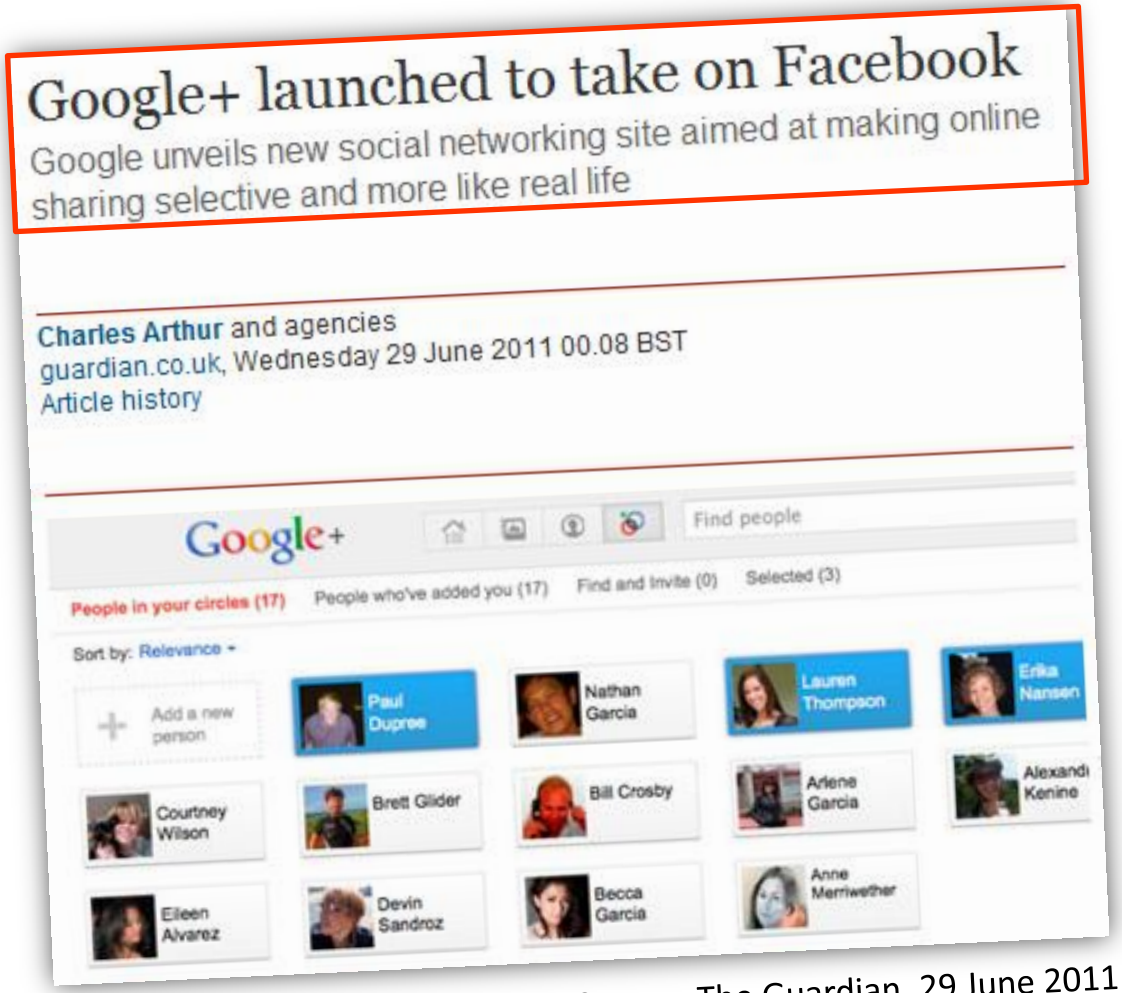
Vietnam: Social Networks

- **Vietnam has the highest year over year growth in reach**

Source: comScore Media Matrix, December 2010

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Social Networks



Google+ launched to take on Facebook

Google unveils new social networking site aimed at making online sharing selective and more like real life

Charles Arthur and agencies
guardian.co.uk, Wednesday 29 June 2011 00.08 BST
Article history

Google+

Find people

People in your circles (17) | People who've added you (17) | Find and invite (0) | Selected (3)

Sort by: Relevance

Add a new person

Paul Dupree | Nathan Garcia | Lauren Thompson | Erika Nansen

Courtney Wilson | Brett Glider | Bill Crosby | Arlene Garcia | Alexandr Kenine

Eileen Alvarez | Devin Sandroz | Becca Garcia | Anne Merriwether

Source: The Guardian, 29 June 2011

facebook

YouTube

tumblr.

LinkedIn

flickr

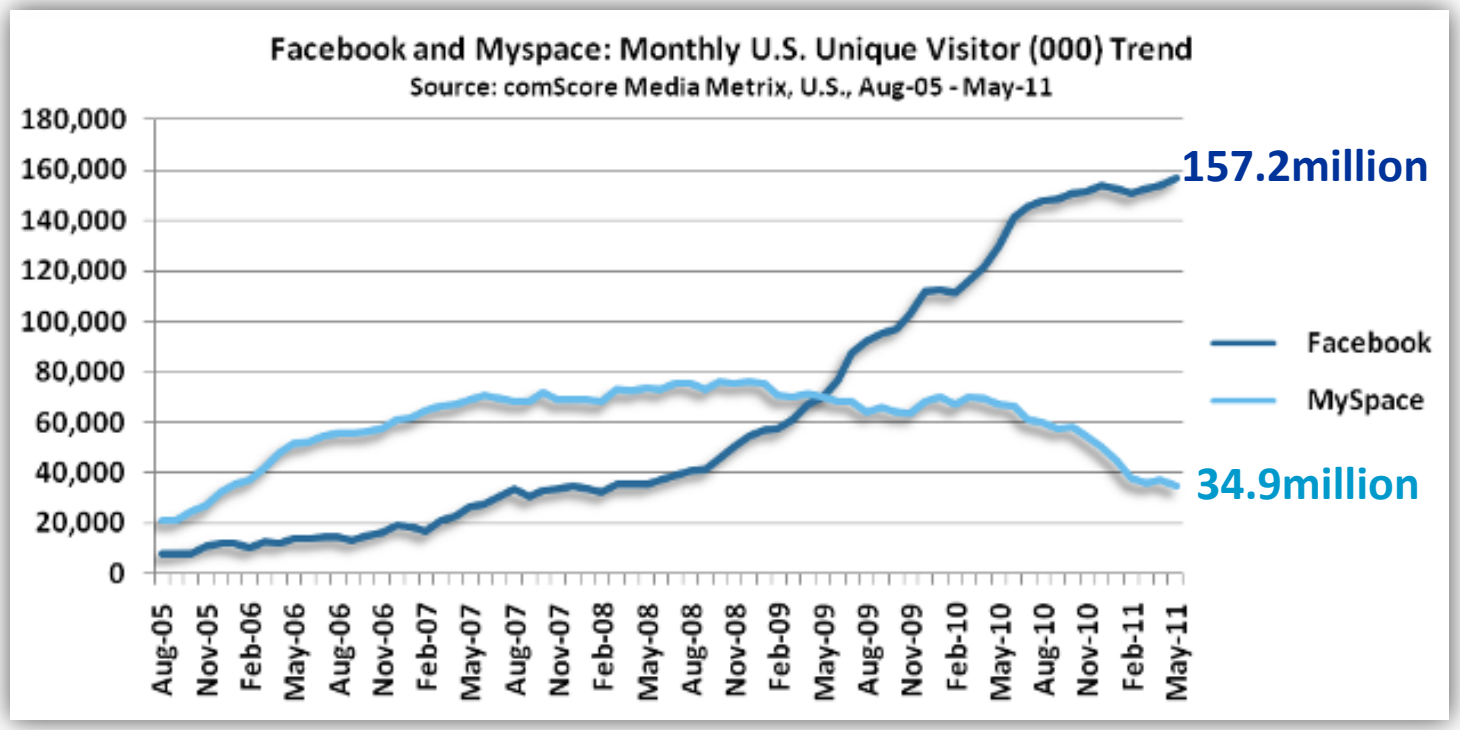
and many more…

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Social Networks

- **More online time is spent on social networking**
  - ✓ 1 out of 12 minutes in 2007 VS **1 out of 6 minutes today**

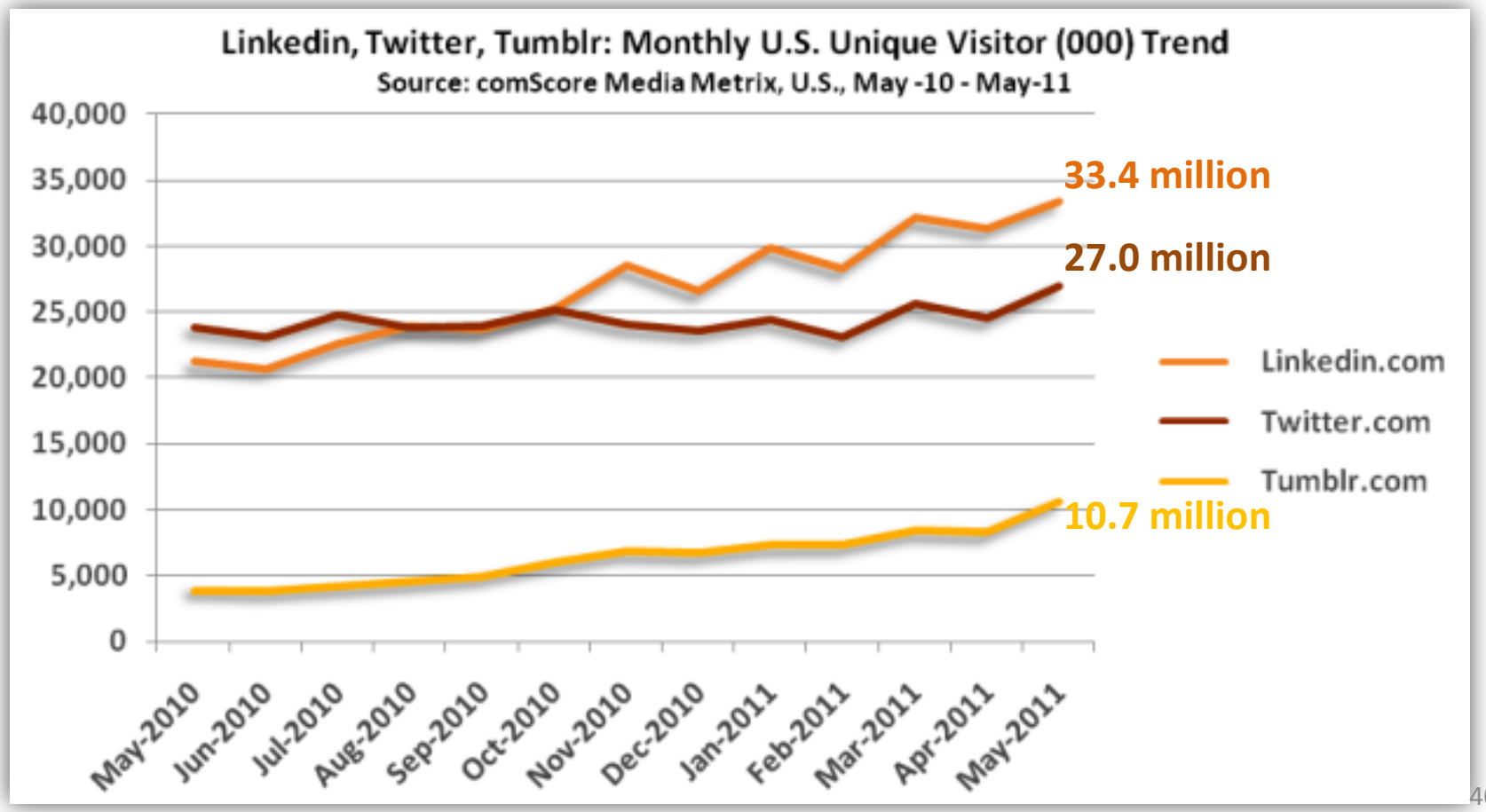
(Source: comSource, 15 June 2011)



Source: comScore's May 2011 US Data

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Social Networks



Source: comScore's May 2011 US Data

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Security Concerns on Social Networks

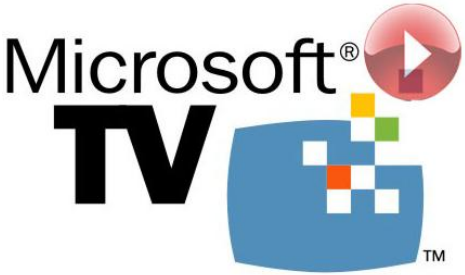
- **Data Leakage**
  - ✓ Intelligence gathering from Social Networks – Twitter, Facebook etc.
- **Social Engineering**
  - ✓ Accessing personal & professional information via impersonation

- **Malicious Applications**
  - ✓ E.g. installing seemingly harmless Facebook applications can deliver malicious content to computers
- **Spam Hoaxes**
  - ✓ Mass-mailing worm in attachments

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Internet TVs

- Investments in Internet TV by big organisations:



- **Global shipments of Internet TV expected to grow to 118 million by 2014** (Source: worldtvpc, 19 December 2010)

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Security Concerns on Internet TVs

Security risks arising from Social Networks

❖Security vulnerabilities in Internet TVs can lead to:

- ✓ Phishing
- ✓ Data theft & unauthorised access
- ✓ Loss of online privacy

❖Example: Researchers from Mocana recently discovered that they could easily hacked into a best-selling Internet-ready HDTV model

Copyright 2000-2011 e-Cop. All rights reserved worldwide.

Q & A

THANK YOU

DISCLAIMER STATEMENT

The e-Cop logo enclosed in each slide is the property of e-Cop. All other marks/logos are the property of the respective owners. The listing of any company or their marks/logos is not intended to imply any endorsement of or affiliation with e-Cop.

Copyright 2000-2011 e-Cop. All rights reserved worldwide.