Universitas Esa Unggul

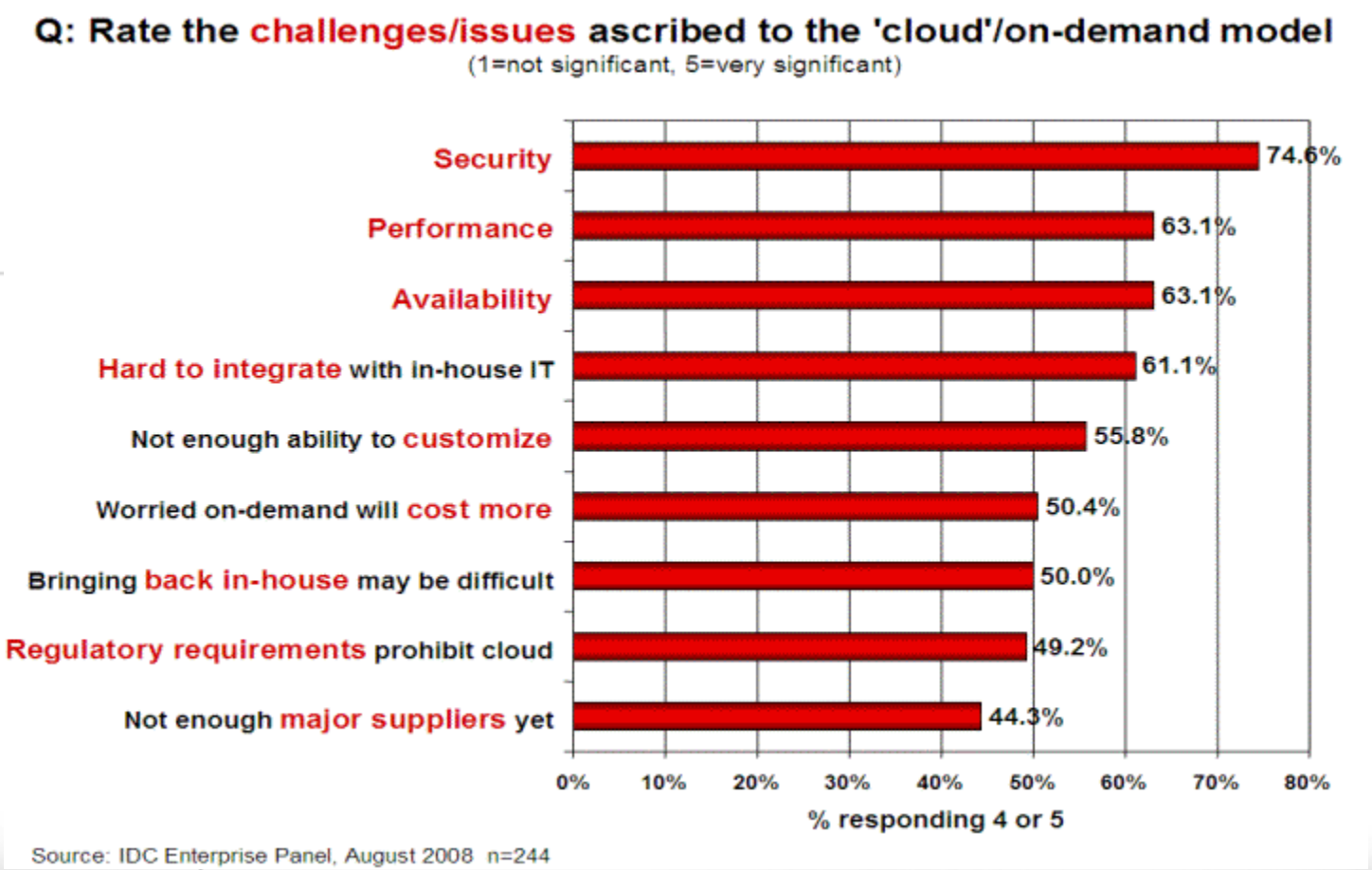
Smart, Creative and Entrepreneurial

www.esaunggul.ac.id

Cloud Computing Security

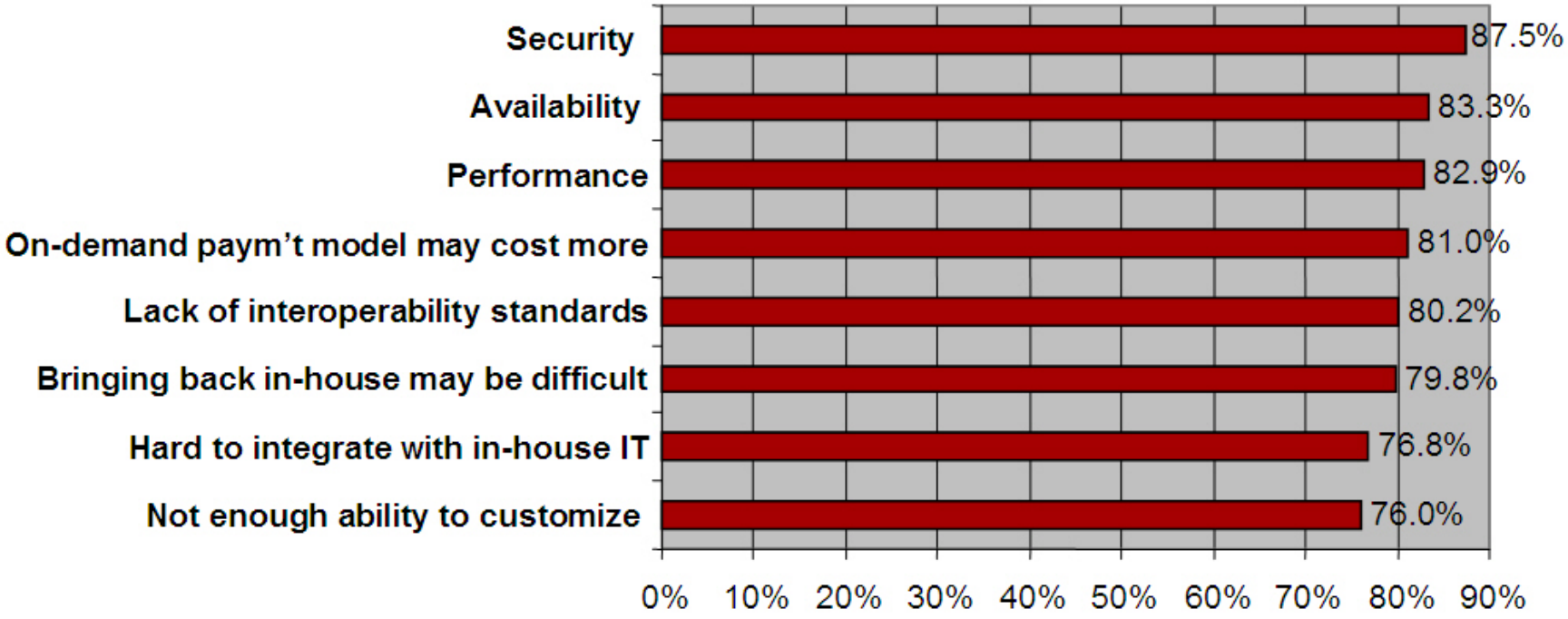
Haditya L. Mukri
Prodi RMIK & MIK

Survey Tantangan Cloud Computing



"The number one concern about cloud services is *security*."

Frank Gens, IDC, Senior VP & Chief Analyst



Source: Source: IDC eXchange, "New IDC IT Cloud Services Survey: Top Benefits and Challenges," (http://blogs.idc.com/ie/?p=730)

Cloud Computing Security

- Cloud Computing Security = IT/Network Security secara umum.
- Jadi semua jenis ancaman atau serangan yang ditemukan pada sistem “tradisional/konvensional”, masih tetap menjadi ancaman pada Cloud Computing. Misalnya Web Security Vulnerabilities yang disebut pada OWASP mulai SQL injection, cross site scripting (XSS), cross site request forgeries (CSRF), dll.
- Penyadapan, scanning, remote exploit, brute force dll juga masih bisa terjadi. Ancaman keamanan fisik juga masih tetap sama, karena bisasa jadi akses oleh pihak pihak yang tidak terotorisasi, hanya saja mungkin sudah menjadi tanggung jawab provider untuk bagian pengamanan fisik tersebut.

Cloud Computing Security

- Pada Prinsip IT Security, terdapat 3 yang menjadi objectives dasar yakni“C” “I” “A”
  - Confidentiality
  - Integrity
  - Availability
- Tantangan paling besar pada cloud computing saat ini adalah “Availability”
- Hampir setiap provider Cloud memberikan jaminan “Availability” yang tinggi pada client.

Cloudflare reveals details o cyber attack

Open DNS recursors are a problem

By **Egan Orion**

Thu Mar 28 2013, 10:26

IN
Clo
ab
Sp
ne

In
Clo
ev
Sp
an attack against its spam blocking service t
gangs" in Eastern Europe and Russia at the b
Cyberbunker.

Cloud Computing di Indonesia Rentan Serangan DDoS

Achmad Rouzni Noor II - detikinet

Senin, 12/03/2012 15:39 WIB

Ilustrasi (Ist.)

Jakarta - Salah satu tantangan dalam menjalankan cloud computing di Indonesia adalah menjaga keamanan data pelanggan. Terlebih, Indonesia ada di posisi nomor dua untuk negara yang sering diserang Distributed Denial of Service (DDoS).

Tak pelak, cloud yang sedang merangkak tumbuh perlu perlindungan keamanan yang maksimal. Apalagi, cloud diyakini bakal menjadi primadona di semua sektor, mulai dari enterprise hingga kalangan usaha kecil dan menengah (UKM).

Bagi perusahaan jasa keamanan internet, kondisi ini justru jadi peluang emas. Itu sebabnya, perusahaan CQ Cloud yang didirikan di Korea Selatan dengan basis operasi di Amerika Serikat, tak ragu-ragu menjejakkan kakinya di Indonesia.

"Kami baru saja mendirikan CQ Cloud Indonesia beberapa minggu lalu," ungkap CEO CQ Cloud, Heon Soo Rhee di Jakarta, Senin (12/3/2012).

Cloud services coming under increasing DDoS attack

News James Stirling, January 29, 2013

New report sheds light on cyber criminals targeting cloud-based infrastructure

Cloud services and data centres are coming under increasing attacks from hackers and defending such infrastructure against the bad guys remains an uphill struggle.

DDoS threats are changing from clumsy battering rams into sophisticated, long-lived, multi-vector attacks, according to the eighth Worldwide Infrastructure Security Report by IT security firm Arbor Networks.

Nearly half of research respondents experienced DDoS attacks targeted at their data centres during the survey period.What's more, some 94 per cent of these respondents reported seeing DDoS attacks regularly.

As more companies move their services to the cloud, they now have to be wary of the shared risks and the potential for collateral damage, according to Arbor

Ancaman Keamanan dari Cloud Computing

- “Cloud Computing” membawa ancaman baru untuk Keamanan
- Pada sistem keamanan sistem server konvensional (tradisional), umumnya yang dijaga adalah agar penyerang tidak dapat masuk ke dalam sistem
- Untuk itu penyerang (attacker) harus mampu menyusup dengan berbagai serangan pada otentikasi atau otorisasi/access control, atau mendapatkan secara ilegal account user lain.
- Sedang pada “Cloud Computing”, attacker yang dapat bertindak sebagai pelanggan yang juga memiliki hak atau akses ke mesin yang sama dengan target

Ancaman pada Cloud Computing

- Permasalahan Confidentiality
- Perilaku/attitude yang tidak baik dari pihak Provider
- Memahami resiko yang ada pada setiap industri yang mempraktekkan sistem oursourcing
- Provider dan Instrastrukturnya membutuhkan kepercayaan

Beberapa jenis serangan dan ancaman baru

- Ancaman-ancaman baru bertambah dari sesama pelanggan
- Server Virtualisasi pelanggan dan attacker dapat ditempatkan pada fisik mesin yang sama
- Serangan kolaborasi(DoS)
- Pemetaan internal cloud infrastructure
- Mengidentifikasi lokasi target Server Virtual target
- Cross-VM side-channel attacks
- Menggali informasi dari target pada mesin yang sama

HIDS (Host Intrusion Detection System)

- Meski infrastruktur Server menggunakan Cloud provider, bukan berarti kita menjadi tidak aware dalam keamanan sistem.
- Sebaiknya tetap memasang lapisan-lapisan keamanan seperti Host IDS
- Open Source HIDS seperti OSSEC (Ossec.net) mendukung aplikasi Cloud seperti VmwareESX

- Sumber : Josua M Sinambela, M.Eng CEH, CHFI, ECSA|LPT, ACE, CCNP, CCNA, CompTIASecurity+