ACA@UBC 2011 International Symposium & Seminar

Social You
How Your Next Text Could Be A Pretext

February 10, 2011

New Urban Protective Analysts

The Social Network Landscape

New Urban Protective Analysts

New Urban Protective Analysts

+ Social Bookmarking Sites

New Urban Protective Analysts


LittlePeopleMeet.com
FAT Dating Service
Online Dating
PlentyOfFish
Free Online Dating
LatinRomantico.com
CONNECTING LATINOS WORLDWIDE
JewishCafe.com
eHarmony
Canada
Short Passions
Black Dating Network
meeting that special someone just got easier
BIG WHERE IT COUNTS
www.under-five-eight.co.uk
match.com
Muslima.com
International Muslim Matrimonials
New Urban Protective Analysts
LargeFriends.com

Investigating Journalism/Leaks

New Urban Protective Analysts

Deployment on Mobile Devices

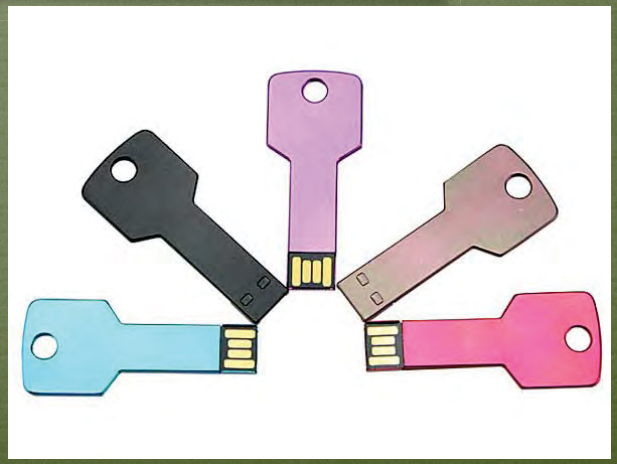
New Urban Protective Analysts

Broadcasting It All Through The Air

New Urban Protective Analysts

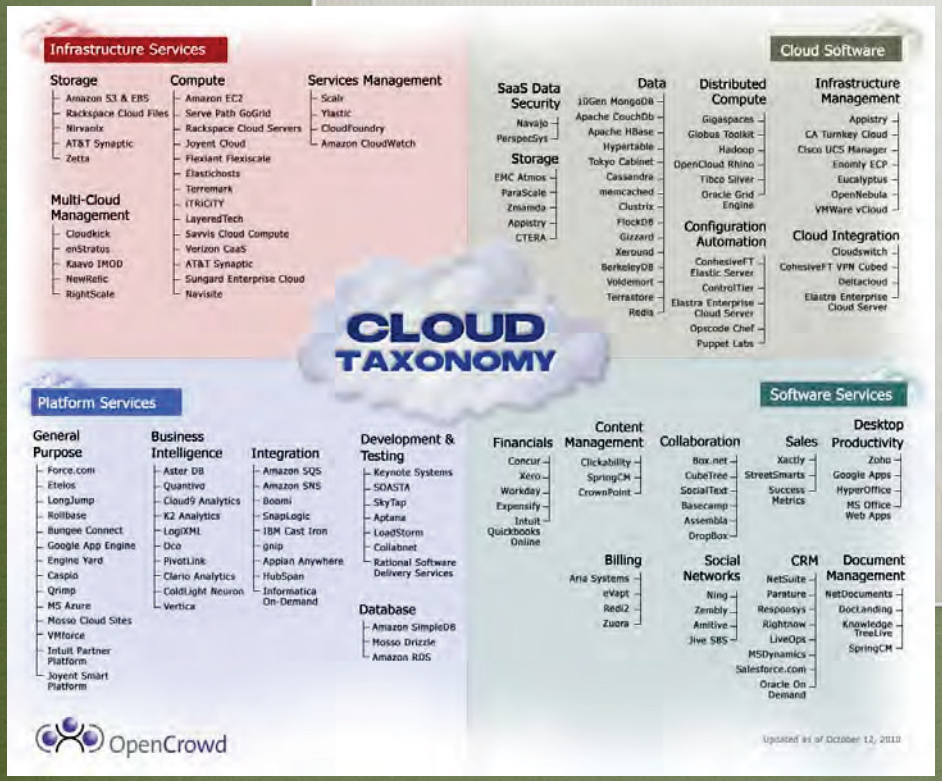
New Urban Protective Analysts

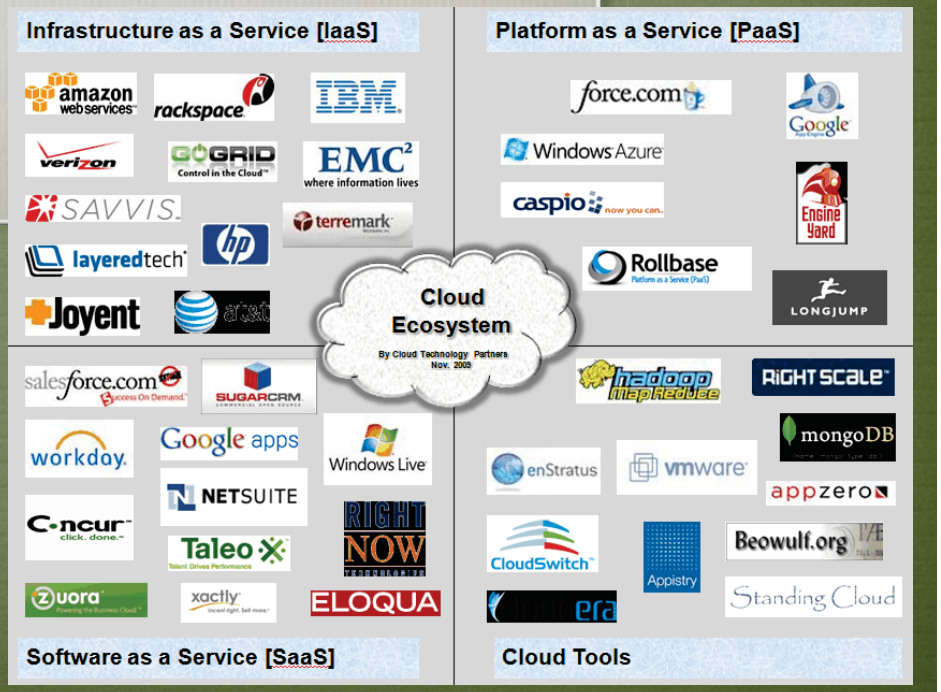
Able to Carry This Information Everywhere



New Urban Protective Analysts

The Cloud





New Urban Protective Analysts

So How Safe Is All This - Really?

New Urban Protective Analysts

New Urban Protective Analysts

Traditional IT & Physical Security

- Ongoing Risk Assessments
- Firewalls
- SPAM Filters
- Antivirus
- Patches
- Intrusion Detection Systems (IDS) & Incident Logging
- Group Policies (Security Policies)
- Access Control List (ACL)
- Physical Security
  - Classification of Data & Documents with Security Markings
  - Locks & Mechanical Hardware
  - Access Control (door access)
  - Intrusion Detection System (alarm system)
  - Closed Circuit Television (CCTV)

Social Engineering – A Big Internal Threat

Definition From Wikipedia:

The act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques.

While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

All social engineering techniques have their basis in **"cognitive biases"** – bugs found in the human decision-making process.

New Urban Protective Analysts

Cognitive Bias

A flaw in judgment caused by memory, social attribution or statistical error.

New Urban Protective Analysts

Types of Cognitive Biases

Decision-Making & Behavioral Biases

"Anchoring Bias"
Heavy reliance on one trait or single piece of information.

Types of Cognitive Biases

Social Biases

"Illusory Superiority"
Overestimate one's desirable qualities, and underestimating undesirable qualities, relative to other people.

Types of Cognitive Biases

Memory Errors

"Suggestibility"

Ideas that someone suggests are mistaken for memory. One thinks they remember facts about what this person suggests.

Social Engineering Techniques

Pretexting

- A story or role-play to engage the victim
- Many times involved impersonation
- Sounds "official" or speaks with "authority"
- Look like they belong in the environment

Fairly Recent Well-Known Example

2006 – Hewlett Packard (HP) General Council and HP chairwoman hire PI firm to investigate board members and journalists to trace source of information leaks. Investigators impersonated HP Board members and nine reporters in order to obtain their phone records.

Social Engineering Techniques

Convicted Hacker Turned Security Consultant Kevin Mitnick

New Urban Protective Analysts

Social Engineering Techniques

Diversion Theft

- Sometimes involves company/security uniform
- UPS, FedEx, etc. are convinced that a legitimate delivery is urgently needed around the corner or nearby
- Variation used to involve Friday evening bank business deposits. Guard, security van & "Night Safe Out of Order"sign.

Social Engineering Techniques

Innocent Picture Taker

- Looks like innocent photographer
  - Uses photos for future access
  - Intelligence Gathering - Sensitive Facilities
- Use of cell phones in secure areas
  - Cameras & Video on every phone
  - Your cell phone can be controlled remotely

Social Engineering Techniques

Cell Phone Vulnerabilities

New Urban Protective Analysts

Social Engineering Prevention

Security Awareness Training, Policies & Procedures

- It's OK to challenge strangers in your area for ID, etc.
- System Admin will not call you to change Your password
- Take a name and phone number
- IT's OK to clear request with your manager and call back
- Refresher training for managers

Technology

- System prompt to change password regularly

Ongoing Re-Training & Penetration Testing

Classify and mark data and documents

Cell phone lockers outside restricted areas

Lock documents and data up - Clear Desk Policy

Build An Environment of Security Every Day

New Urban Protective Analysts

Questions?

Joe Zaccaria
Managing Director
New Urban Protective Analysts

1-866-459-0665
joezac@mac.com

Additional Research

People Threats

- 80% Corporate Vulnerabilities Are Internal (?old FBI stat)
- July, 2010 – US Secret Service and Verizon Report[1]
  - 900 Breaches and 900M compromised records
  - 69% data-loss incidents = outsiders (-9% 2009-2010)
  - 49% data-loss incidents = insiders (>50% 2009 - 2010)

1 2010 US Secret Service & Verizon - "Data Breach Investigations Report"

Internal Threats[2]

- A negative work-related event triggered most
- 62% Insider incidents planned in advance
- 80% Insiders exhibited unusual behaviour prior to event
- 39% Used sophisticated attack tools
- 60% Compromised accounts or used backdoor or shared accounts
- Most incidents carried out via remote access
- Less than half (43%) had authorized access at time of incident
- 57% Insiders exploited systematic vulnerabilities in: Applications, Processes & Procedures

2 2005 US Secret Service & Carnegie Mellon's CERT – "Insider Threat Study"

Results of Insider Attacks

- 81% Caused financial losses
- 75% Resulted in negative impacts to business operations
- 28% Damaged the organization's reputation

2 2005 US Secret Service & Carnegie Mellon's CERT – "Insider Threat Study"

Questions?

Joe Zaccaria
Managing Director
New Urban Protective Analysts

1-866-459-0665
joezac@mac.com