Understanding Web 2.0 Security & Privacy Issues

DALE JOHNSTONE
dale.johnstone@pccw.com

Chairman ISMS IUG (Hong Kong / Macau)
Chief Security Officer, Risk Management
PCCW Limited

Communications
Technology
Information

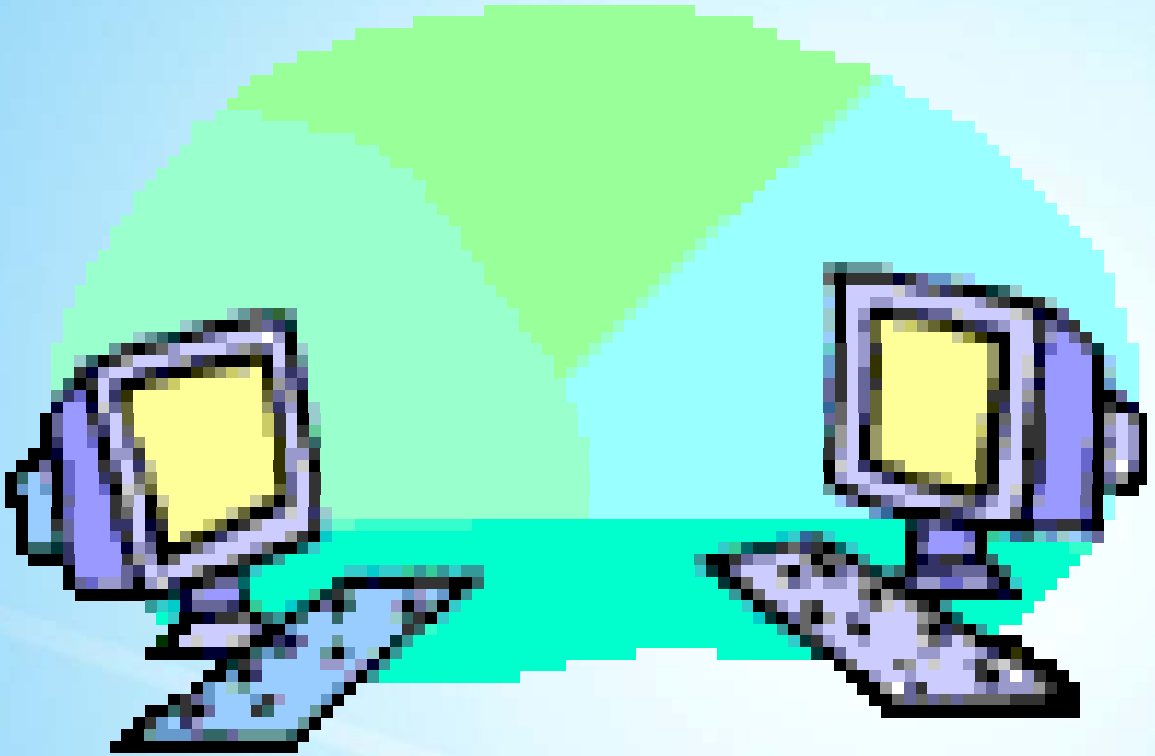
Solutions

2 June 2008

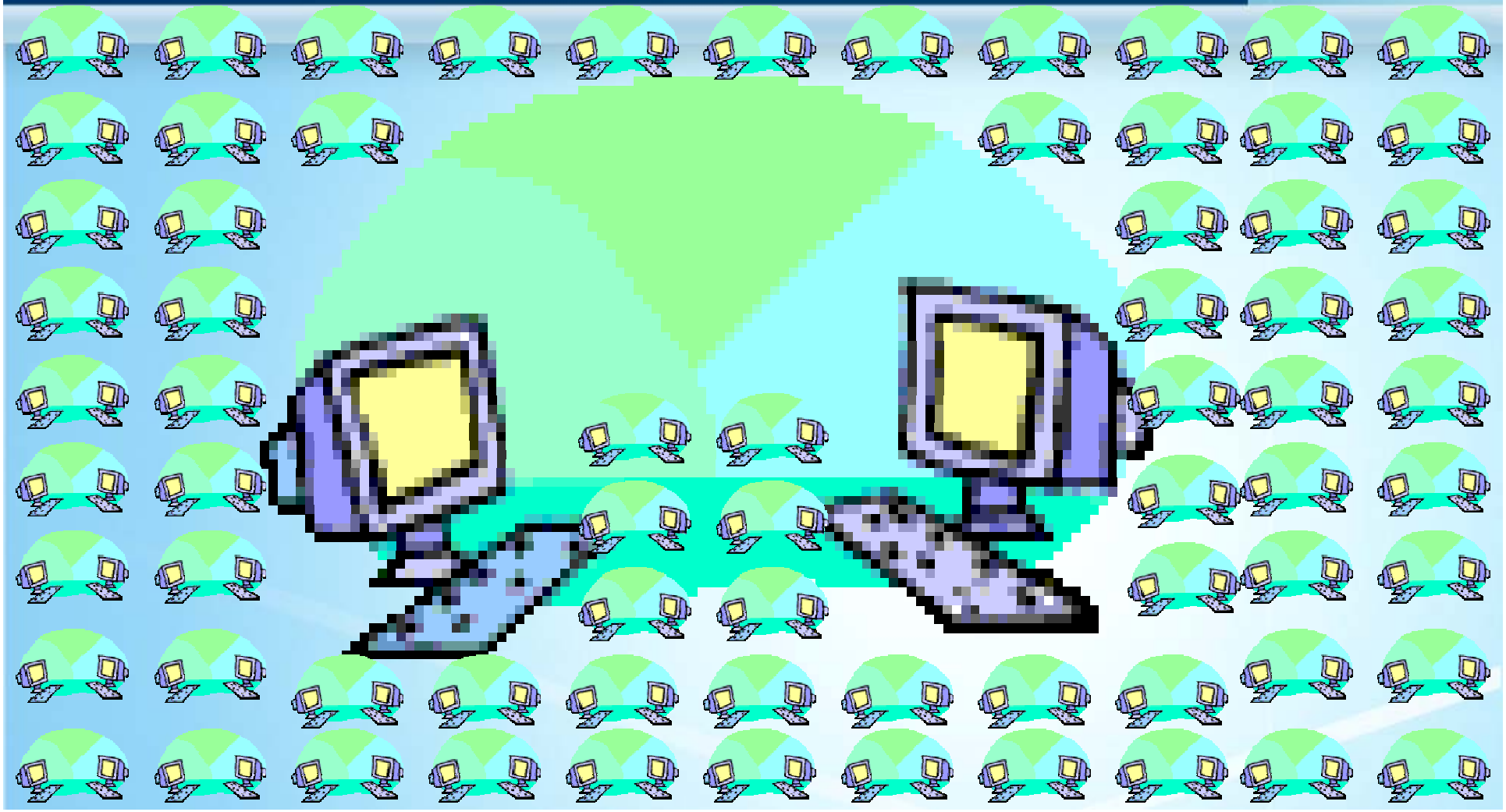
Web 2.0 – Connecting People

1. Amplify Power of People Working Together
2. Integrate Broad Technologies & Social Forces
3. Social Technology Resources Proliferating
4. Mixing Technology with Social Interactions
5. Rapid Development of Interpersonal Interactions

Web 2.0 – Connecting People



Web 2.0 – Connecting People



WEB 2.0 Security Challenges

Well Publicized (FUD)
- **Security Risks**
- **Privacy Risks**

Simultaneous Benefits & Protection – Possible?

Do Positives Outweighed Negatives?

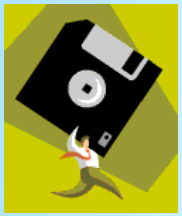
Opportunities - allowing access to:
- **additional sources of everything**

Is it possible to Stay Vigilant ?

WEB 2.0 Security Challenges

New Technologies 

Simple Services (Blogs Wikis) → Complex (mash-ups)



Access to Services & Content Promises to be both:

Inexpensive 

Easy to Compose 

Is WEB 2.0 Security Possible ?

How to secure such a fast moving force?

PEOPLE **PROCESSES**

TECHNOLOGY

Security Issues – Management of:

** TRANSIENT AND LONG TERM RELATIONSHIPS

Privacy

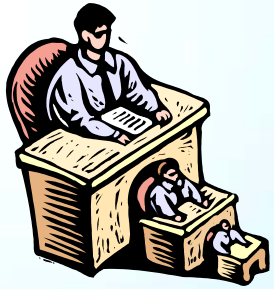
A

Anonymity

Identities

R

Reputation



** COMPOSITION OF FUNCTION AND CONTENT

Security Issues

Not New

Technologies Adopting & Adapting Very Quickly

Being Associated with a Wider Audience

Deliberately Bypassing Traditional Security Mechanisms

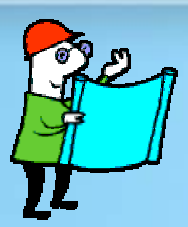
Risks

- **Insider Leakage**
  - **Corporate Gain (Staff Turnover)**
  - **Personal Gain (Extra $)**
- **External Leakage**
  - **Opportunist (Falls into Lap)**
  - **Malicious (Hacking)**
- **Data Corruption**
  - **Malicious (Virus)**
  - **Uncontrolled (Power)**

Risk Mitigation Considerations

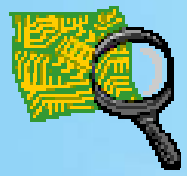
- **Confidentiality**
  - Security Policies & Procedures
  - Access, Authentication & Privilege Controls
  - Encryption
- **Integrity**
  - Data and Malicious Code Filters
  - Reconciliation
- **Availability**
  - Real-Time Monitoring
- **Assurance**
  - Logging, Auditing and Archiving

Risk Mitigation - Best Practices



- **Policy (Plan)**
  - Document Management Intentions

- **Baseline (Do)**
  - Implement Appropriate Controls

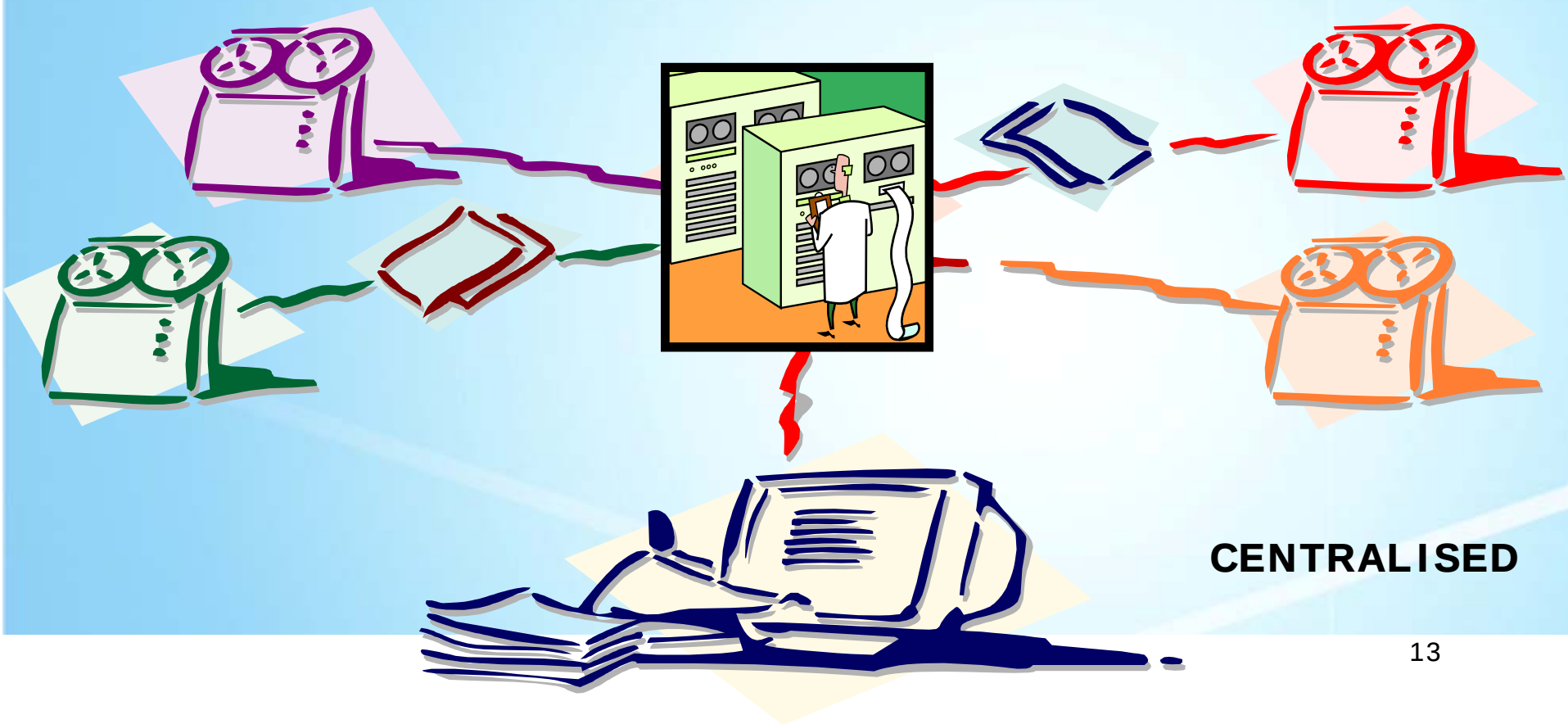


- **Monitoring (Check)**
  - Check for Deficiencies

- **Enforcement (Act)**
  - Security Compliance & Improvement

Corporate Security Solution

Policies - Security and Privacy
Architecture - End-to-End Security



Corporate Security Solution

Policies - Security and Privacy
Architecture - End-to-End Security

DECENTRALISED

Corporate Security Solution

Policies - Security and Privacy
Architecture - End-to-End Security

Consider

Business
Architecture
Security
Monitoring

Case Studies
Extent of Customisation
Ability to Execute
Post Support
Product Life-Cycle

Corporate Security Solution

Policies - Security and Privacy
Architecture - End-to-End Security

Understand Product Security Capabilities

Be Clear About Information You Wish To Share

Determine Security Features You Want

Talk to Trusted People About Their Experiences

Select Product Providing Greatest Benefits

Corporate Security Solution

Policies - Security and Privacy
Architecture - End-to-End Security

Plan, Implement, Check & Update Security Settings

- **Product Directly Reflects Openness**
- **Privacy & Security v. Openness**
- **Decide Extent of Information Lockdown**
- **Public v. Private Profiles**
- **Accessible only to connected friends or Wider**

Corporate Security Solution

Policies - Security and Privacy

Architecture - End-to-End Security

Accountability - Who is Responsible?

Content Composition

- Security of (e.g. Embargo and IPR)
- Style Guide

Versioning

Static Auditing

Dynamic Security Analysis

- Real-Time Security Rules (Admin / User)

Security as a Service (on-going)

User Security Tips – Control:

Your Profile - For Each Site On Each Site

Who Can Contact You

Who Can Find You (i.e. in a Search)

Control What Information They Will Find

Use Progressive Profiles Wisely

- Connect With Someone But Not Share Everything

Consider Privacy

- You Decide Whether or Not People are Notified
  - i.e. when you make changes to your profile
- Whether profiles you visit will know of your visit

User Security Tips – Control:

Be Careful Who You Link To

Implicit Risk in a Sharing Site

Open to Anyone Who Follows The Rules

- **Good People**
- **Bad People (i.e. People With Malicious Intent)**

Control Who You Allow Into Your Network

Always Check Requests From Someone Claiming To Know

- **i.e. Check via Another Connection or Friend**
  - **Ensure it is Legitimate**

Do not accept:

- **Someone Who You Do Not Know**
- **Someone You Have Not Checked Out**

Balance Common Sense With

- **Skepticism per Unknown / Unsolicited Communications**

User Security Tips – Control:

You Are Your Own Worst Enemy Online

Risk Exists That You Will Disclose Too Much Information

What You Post Will Be Exposed to ALL People - Good & Bad

Be Skeptical & Cautious

Lots of Things People Should Not Tell Others - But They Do Anyway

Avoid Social Engineering & Elicitation

- **When someone uses what they know about you to try to learn something about you or your company that is better not disclosed**

Disclose Anything Of Real Concern

Exercise Reasonable Judgment When Deciding What To Disclose

Build Understanding of Trust to Enhance Relationships

Understanding Web 2.0 Security & Privacy Issues

DALE JOHNSTONE
dale.johnstone@pccw.com

Chairman ISMS IUG (Hong Kong / Macau)
Chief Security Officer, Risk Management
PCCW Limited

Communications
Technology
Information

2 June 2008