How can Security Professionals Survive in the Cloud Computing Era?

Prof. Frank Yam

CISA, CIA, FHKCS, FHKIoD, FFA, FIPA, FHKITJC, CFE, CFSA

Chairman & CEO - Focus Strategic Group Inc

© Frank Yam 2016

Warning!!!

- All information discussed in this seminar is the personal opinion of the Seminar Leader and is meant to stimulate new ideas from the participants.
- Under no circumstances should any of the opinion be relied upon for decision making or used for any other purposes.
- The Seminar Leader does not assume any liabilities for the opinion expressed in this seminar.
- Audio, video, or any other form of electronic recording is strictly prohibited.

© Frank Yam 2016

Agenda

Understand Cloud Computing Models and Environment

Benefits and Opportunities

Risks and Challenges

Audit and Control

© Frank Yam 2016

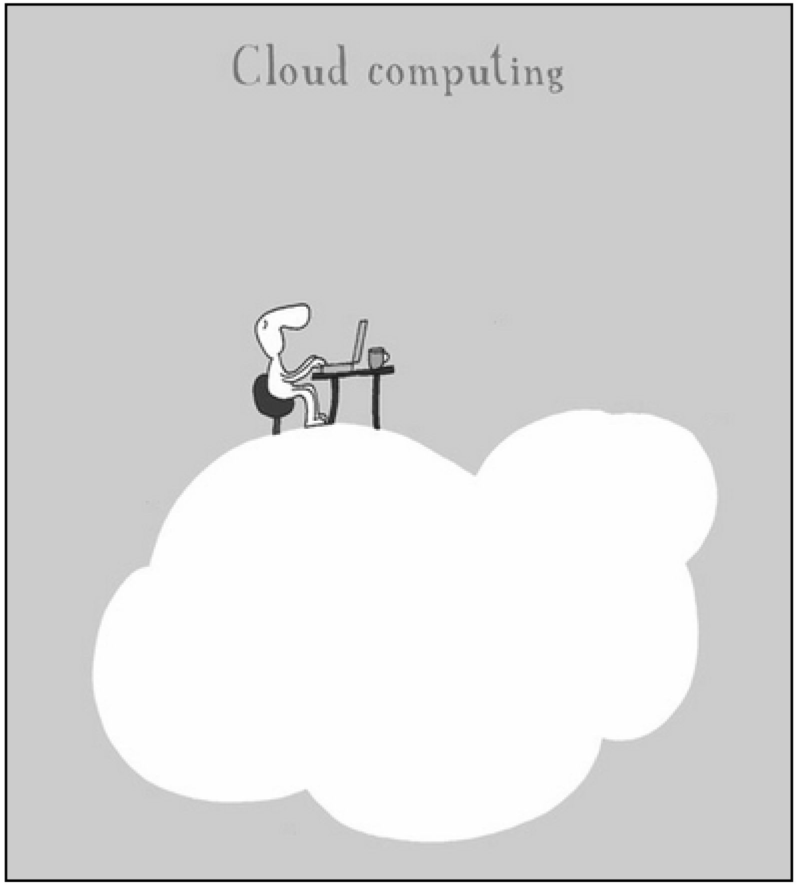
Key Points

- Organisations (and individuals) will rely more and more on Cloud Computing
- We should anticipate more Cloud-related risks (and frauds)
- We will be expected to understand Cloud-related risks and to recommend appropriate controls

© Frank Yam 2016

Understanding Cloud Computing

Understanding Cloud Computing



Question:

Anyone in this room using cloud computing ?

Understanding Cloud Computing

Even if you may not recognize it, you're probably already using cloud computing and are pretty savvy in using it.

Examples:

- web email such as Gmail, Hotmail and Yahoo email;
- social networking sites like Facebook and Twitter
- video streaming sites like youtube
- productivity software sites like Google Docs and Microsoft's Office 365
- file synchronisation and backup services Apple iCloud, Dropbox and Microsoft SkyDrive.

© Frank Yam 2016

Who Started All This?

“What's interesting [now] is that there is an emergent new model, and you all are here because you are part of that new model. I don't think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it **cloud computing** – **they should be in a "cloud" somewhere**. And that if you have the right kind of browser or the right kind of access, it doesn't matter whether you have a PC or a Mac or a mobile phone or a BlackBerry or what have you – or new devices still to be developed – **you can get access to the cloud**.”

Mr. Eric Schmidt, Chairman & CEO Google

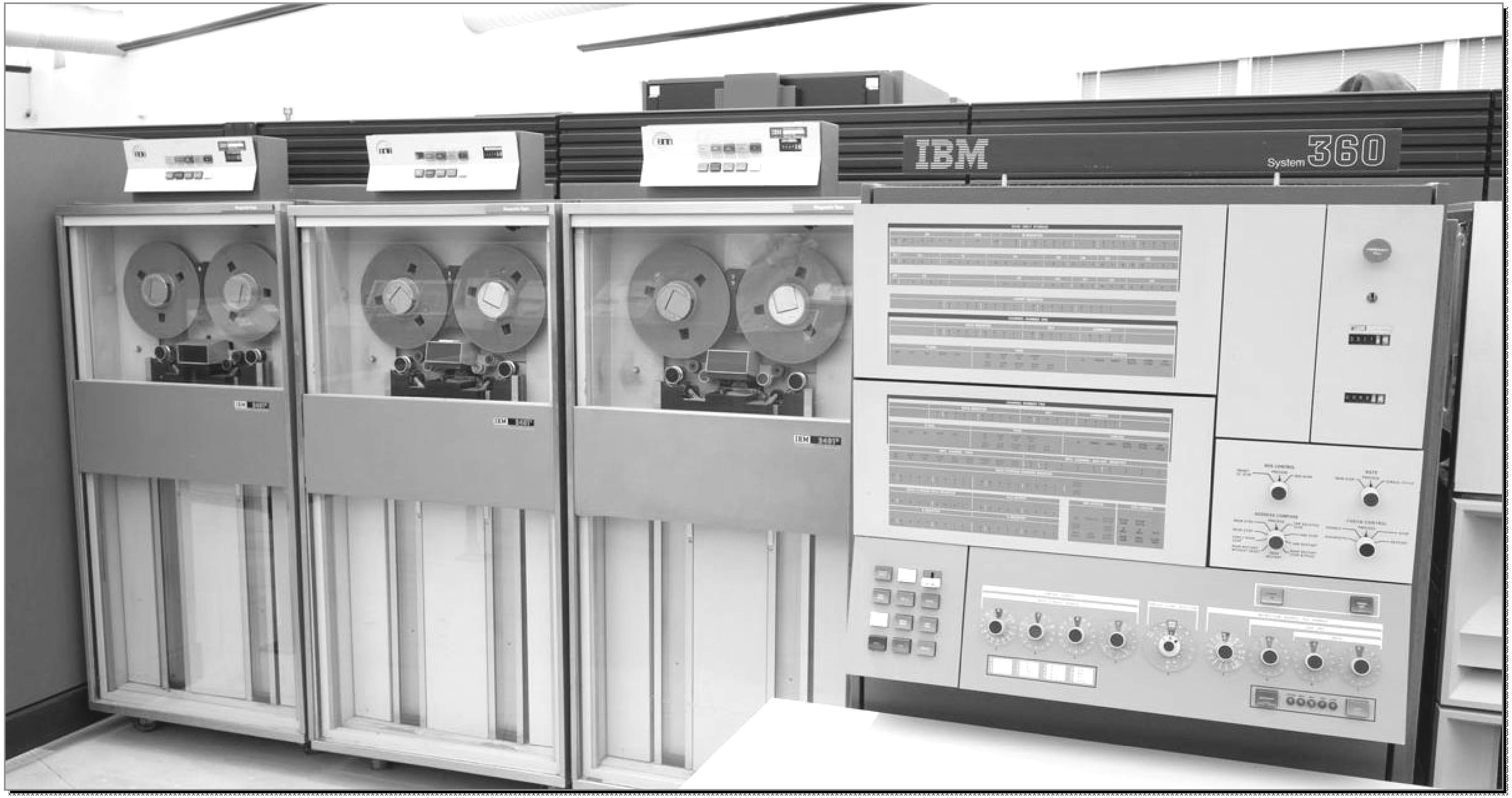
Search Engine Strategies Conference, 9th of August 2006

© Frank Yam 2016

Evolution – "First Computer"

© Frank Yam 2016

Evolution – Mainframe Computer



© Frank Yam 2016

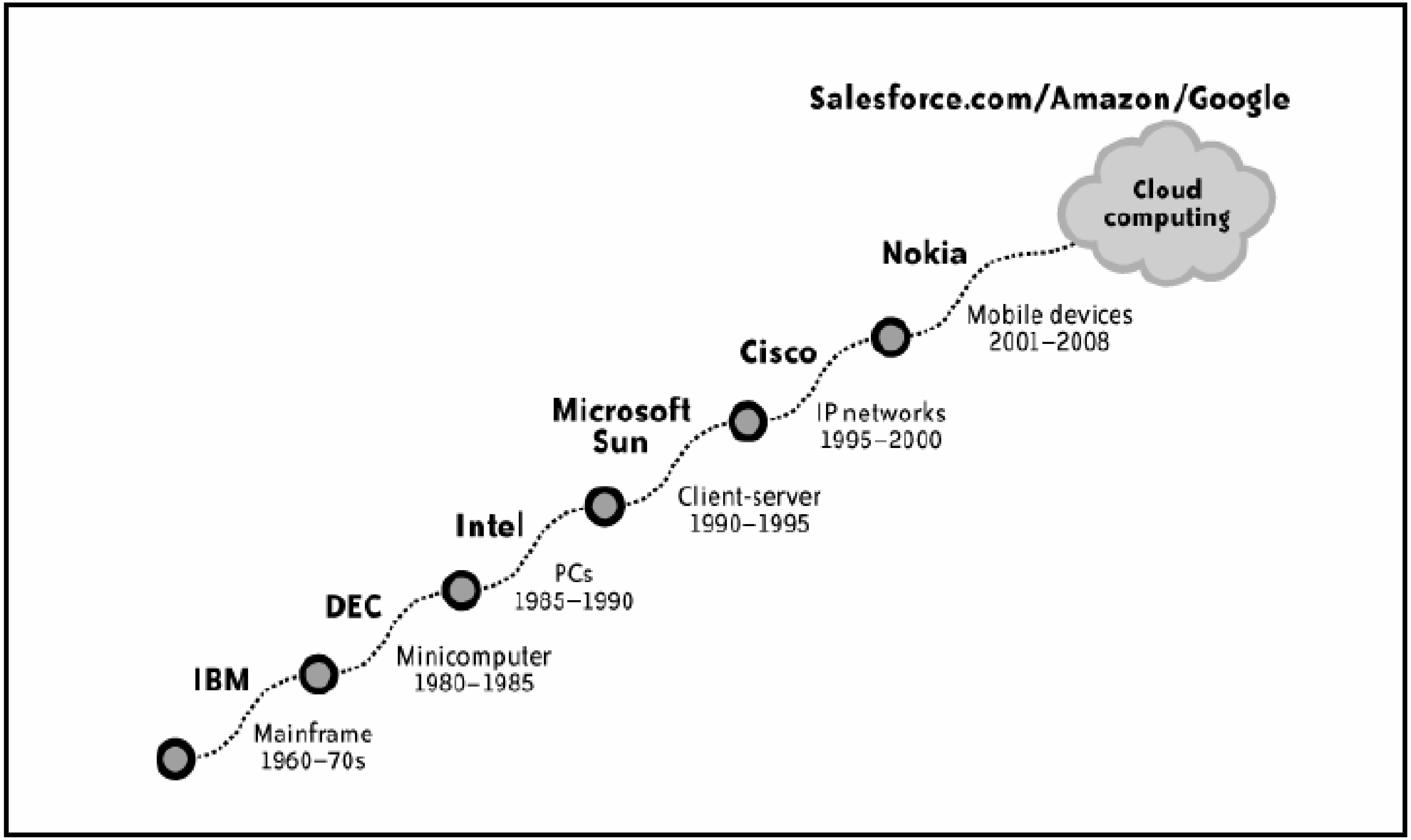
Evolution – Mini Computer, PCs and Internet

Evolution - Cloud Computing

© Frank Yam 2016

Evolution - Cloud Computing

Subwaves within the Information Revolution



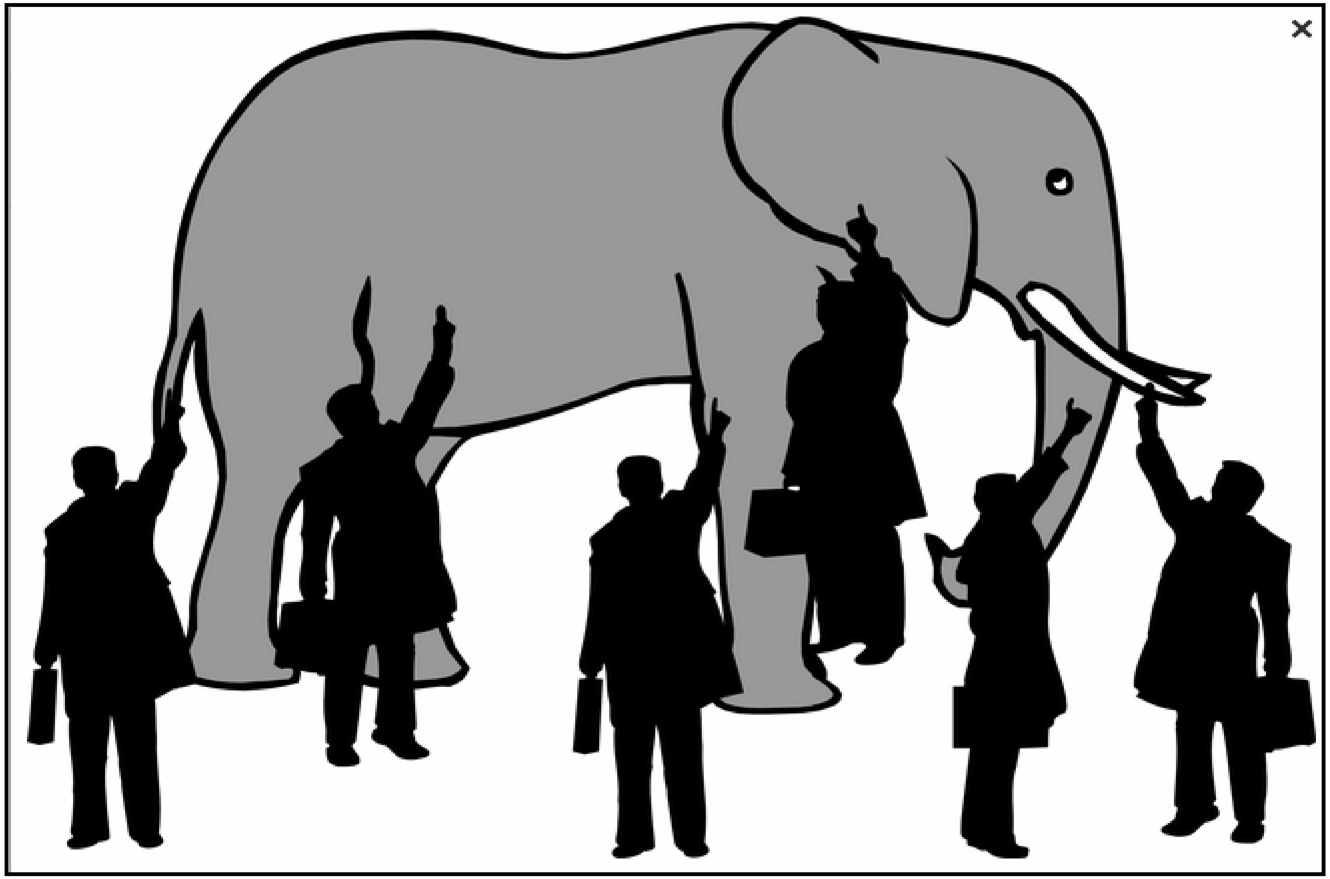
Evolution - Cloud Computing

Computing is being **organized as a public utility** just as the telephone system is a public utility. Likewise, factories used to provide their own power using water wheels. With electrification, factories do not need to produce their own power. They just need to plug into the electricity grid.

Organizations are providing their own computing resources. In future, most organizations will **just plug into the cloud for their computing resources**. The computer utility is becoming the basis of a new and important industry.

Understanding Cloud Computing

So what is cloud computing?



© Frank Yam 2016

Understanding Cloud Computing

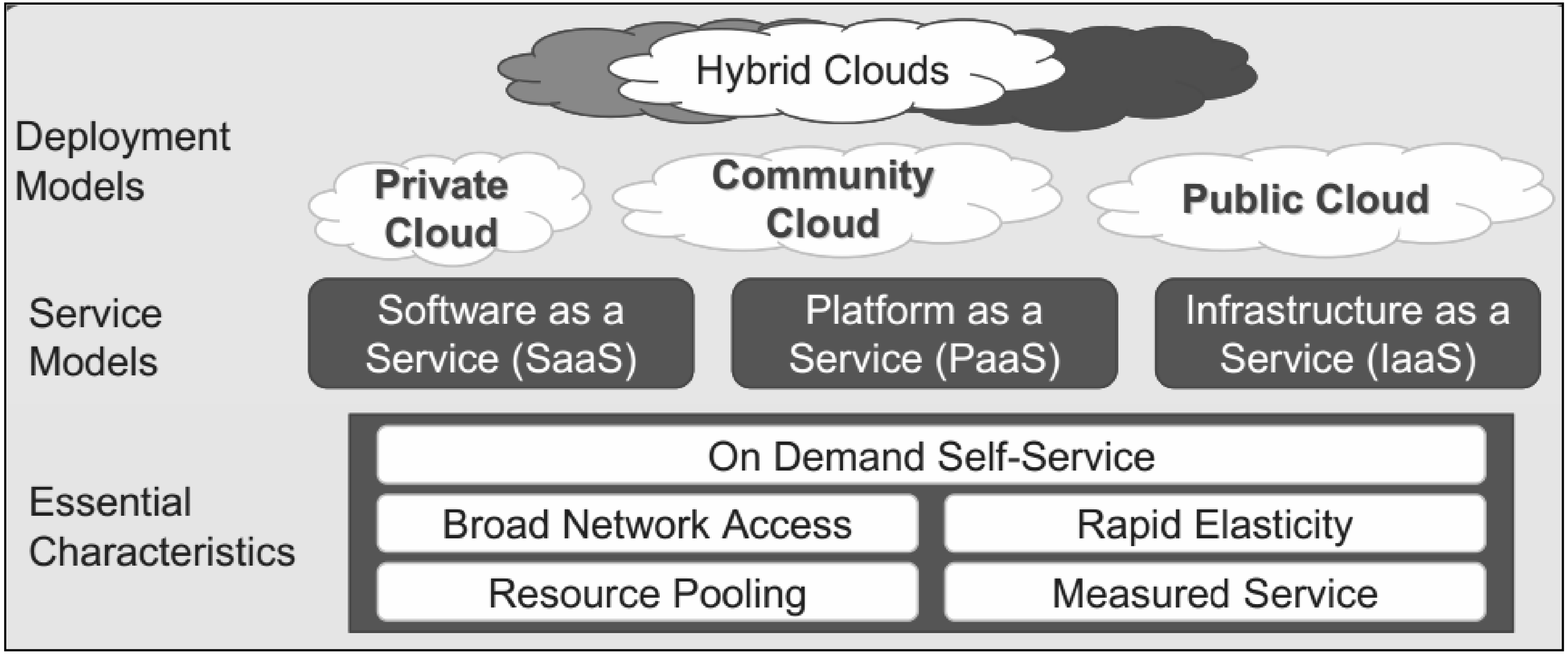
Defining Cloud Computing:

National Institute of Standards and Technology
U.S. Department of Commerce

“*A model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction.*

In layman’s language - Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software and information are provided to computers and other devices as a **utility** (like the electricity grid) **over a network** (typically the Internet).- From Wikipedia

Understanding Cloud Computing
(In Summary)



Hybrid Clouds

Deployment Models

Private Cloud

Community Cloud

Public Cloud

Service Models

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Essential Characteristics

On Demand Self-Service

Broad Network Access

Rapid Elasticity

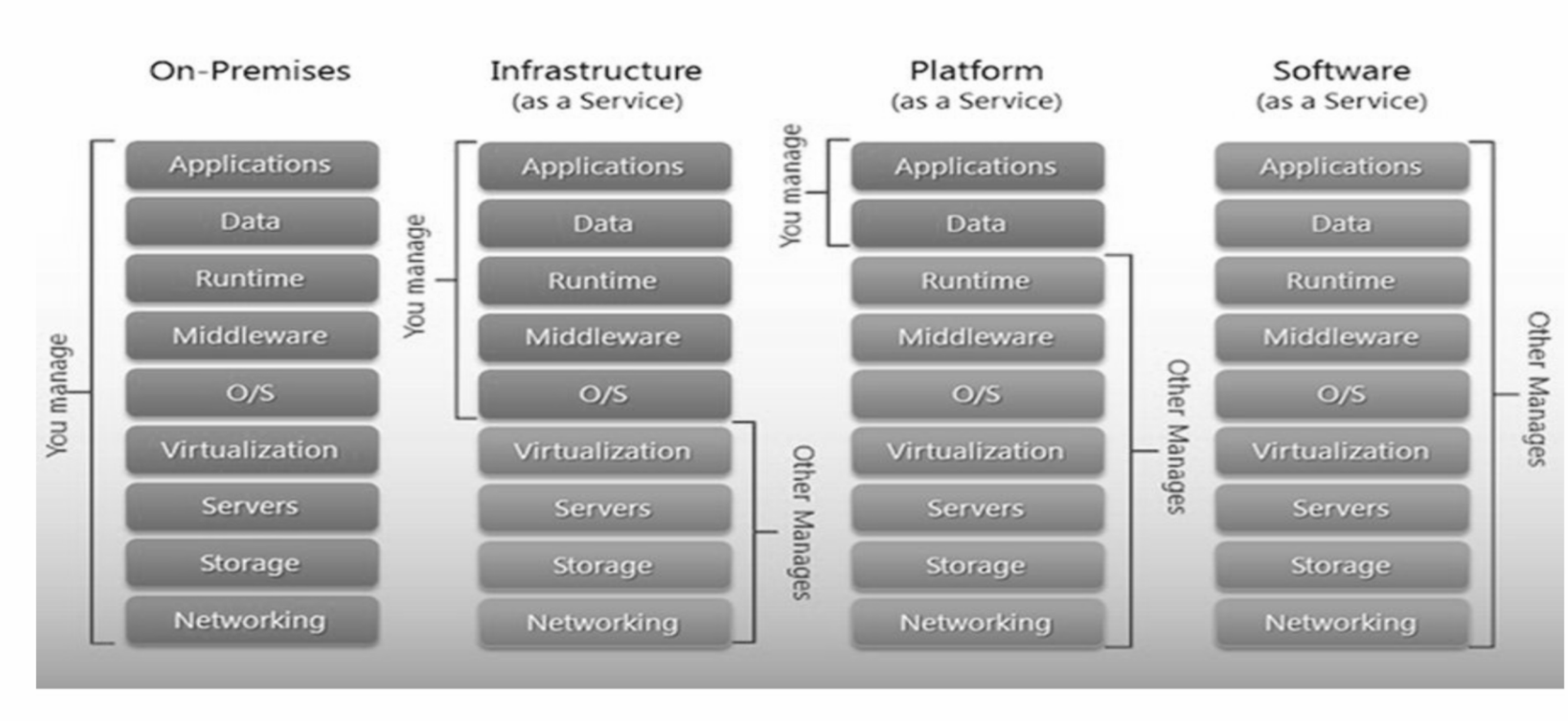
Resource Pooling

Measured Service

NIST Visual Definition of Cloud Computing

© Frank Yam 2016

Sharing of Responsibilities



On-Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

On-Premises: You manage (Applications to Networking)

Infrastructure (as a Service): You manage (Applications to O/S); Other Manages (Virtualization to Networking)

Platform (as a Service): You manage (Applications, Data); Other Manages (Runtime to Networking)

Software (as a Service): Other Manages (Applications to Networking)

© Frank Yam 2016

Understanding Cloud Computing

You will also hear other associated service models in the future, for example:

- Security as a Service (SecaaS)
- Storage as a Service (StaaS)
- Disaster Recovery as a Service (DRaaS)
- Identity as a Service (IDaaS)

© Frank Yam 2016

Benefits and Opportunities

Business Benefits

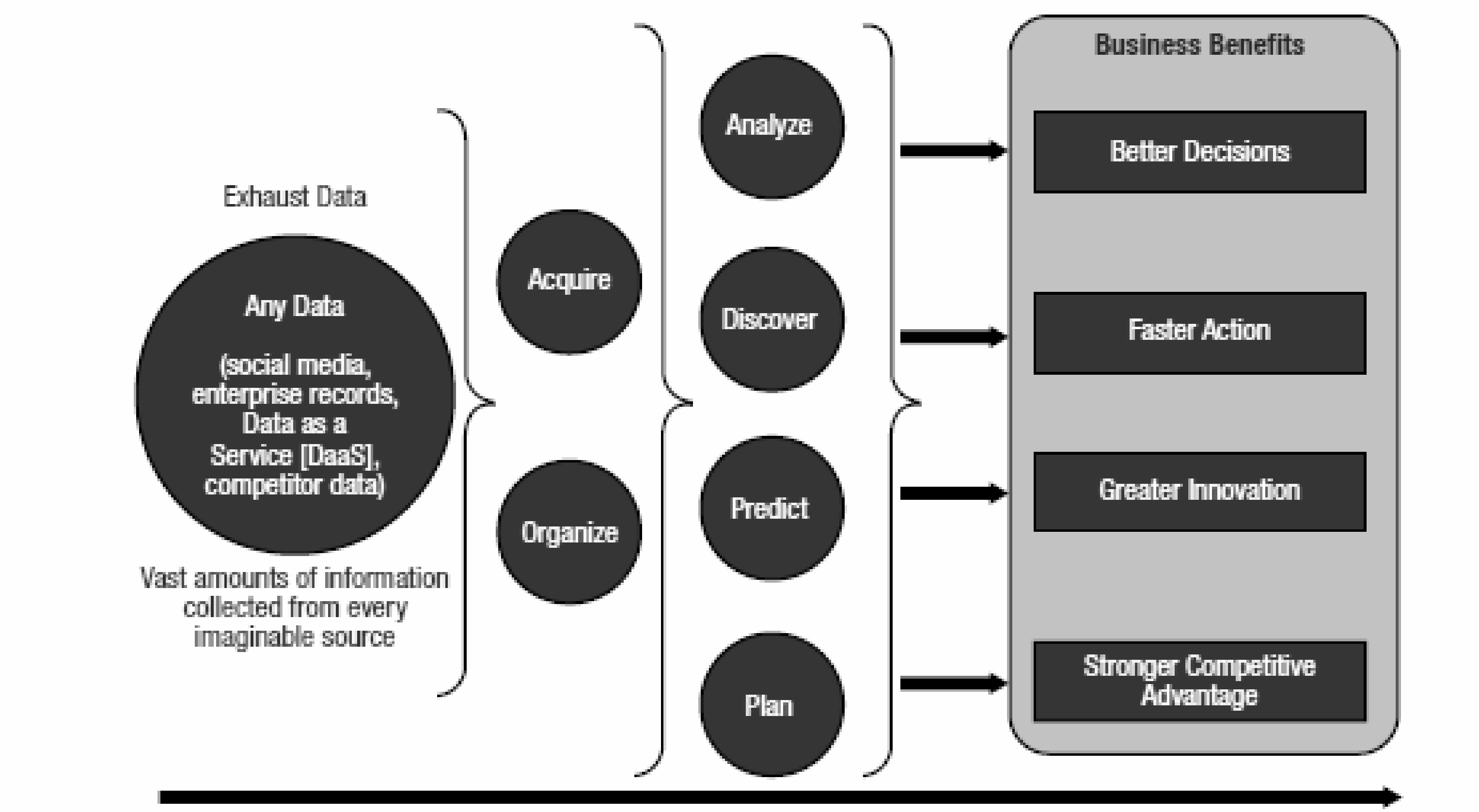
We are finally in sync with the business

Cloud Computing Benefits

- Cost savings (CAPEX to OPEX)
- Optimized resource utilization
- Lower Power Consumption (“green”)
- Speed to Deployment
- Near instant scalability, provisioning
- ‘Service On demand’ (better responsiveness)
- A ‘Pay as you go’ billing system
- Resilience (reduces risk of downtime)

Opportunities
straight ahead

BIG DATA
Business Benefits



Exhaust Data

Any Data

(social media, enterprise records, Data as a Service [DaaS], competitor data)

Vast amounts of information collected from every imaginable source

Acquire

Organize

Analyze

Discover

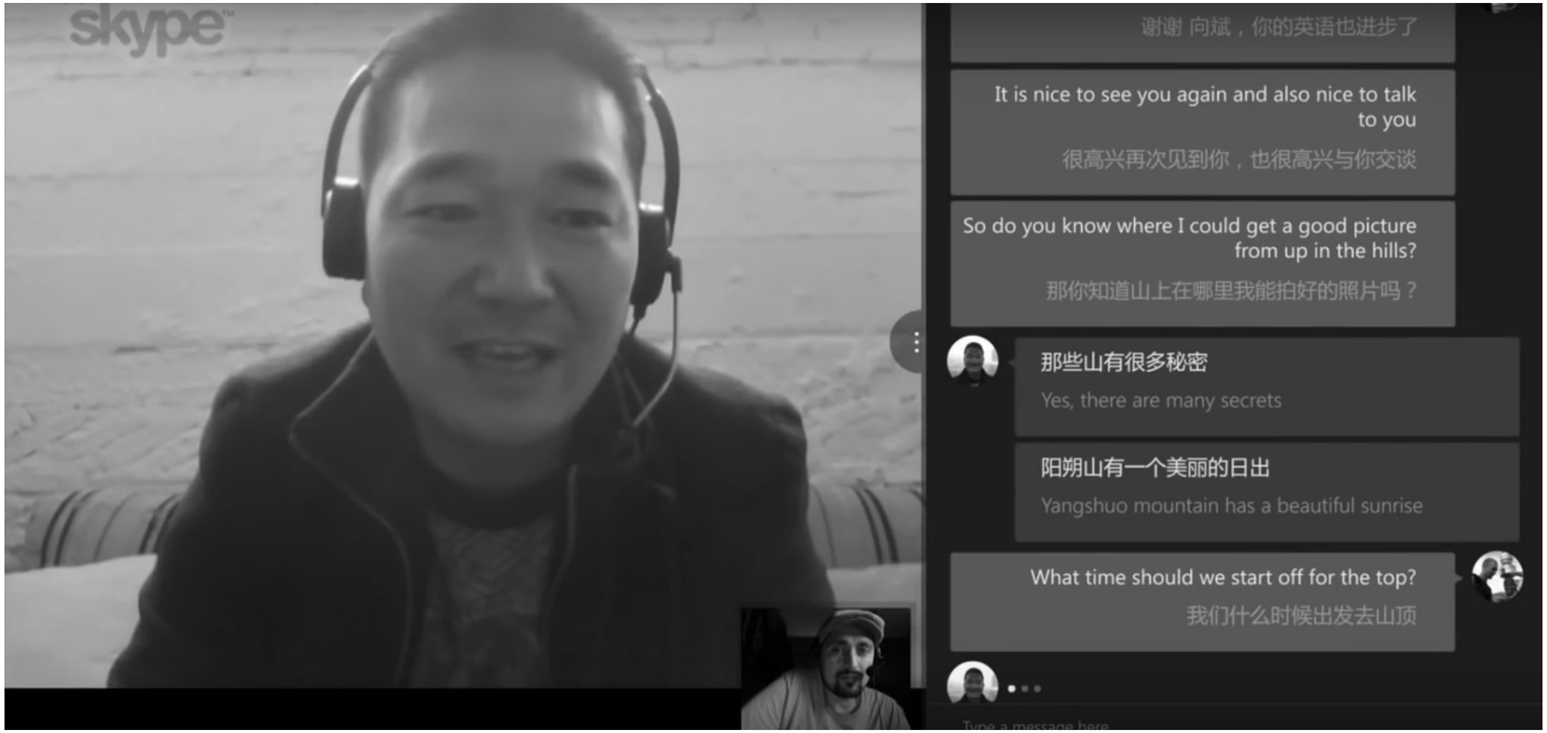
Predict

Plan

Business Benefits

- Better Decisions
- Faster Action
- Greater Innovation
- Stronger Competitive Advantage

Emerging Trends and Predictions
Bridging the language gaps



谢谢 向斌，你的英语也进步了

It is nice to see you again and also nice to talk to you
很高兴再次见到你，也很高兴与你交谈

So do you know where I could get a good picture from up in the hills?
那你知道山上在哪里我能拍好的照片吗？

那些山有很多秘密
Yes, there are many secrets

阳朔山有一个美丽的日出
Yangshuo mountain has a beautiful sunrise

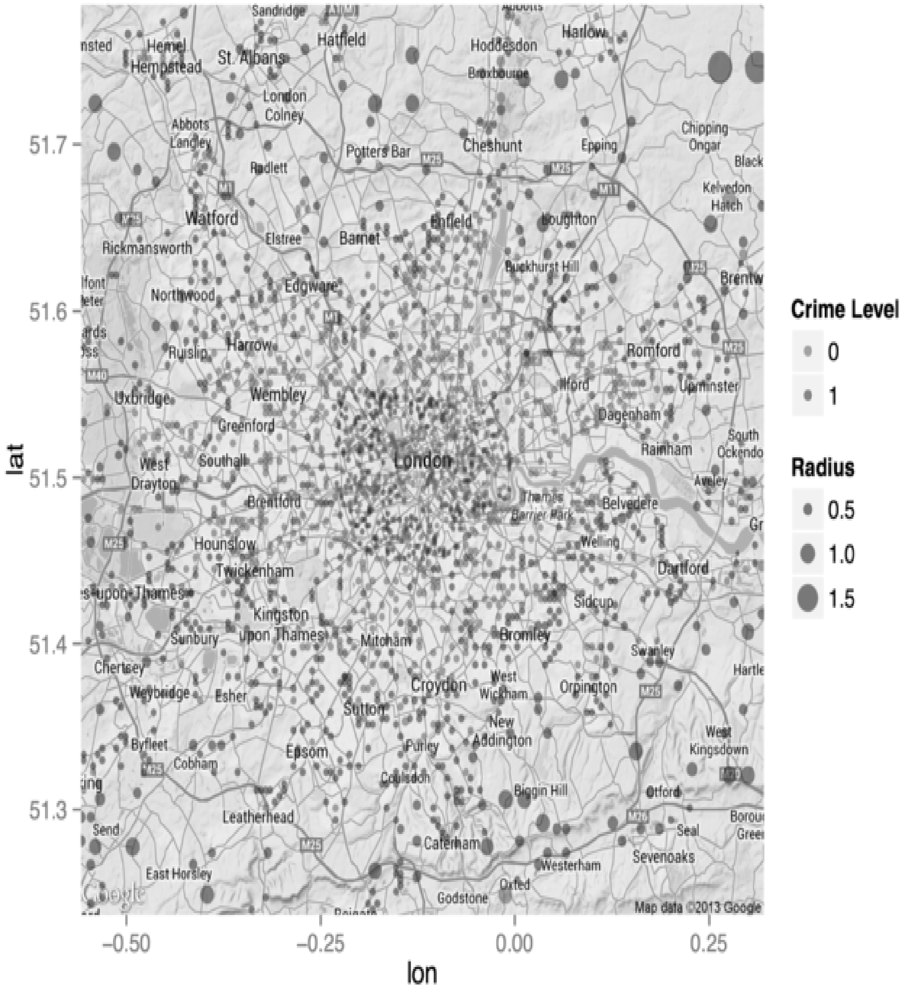
What time should we start off for the top?
我们什么时候出发去山顶

© Frank Yam 2016

Emerging Trends and Predictions
Better Shopping Experience

Emerging Trends and Predictions
Using Big Data to Predict Crime

Crime Hot Spots in London



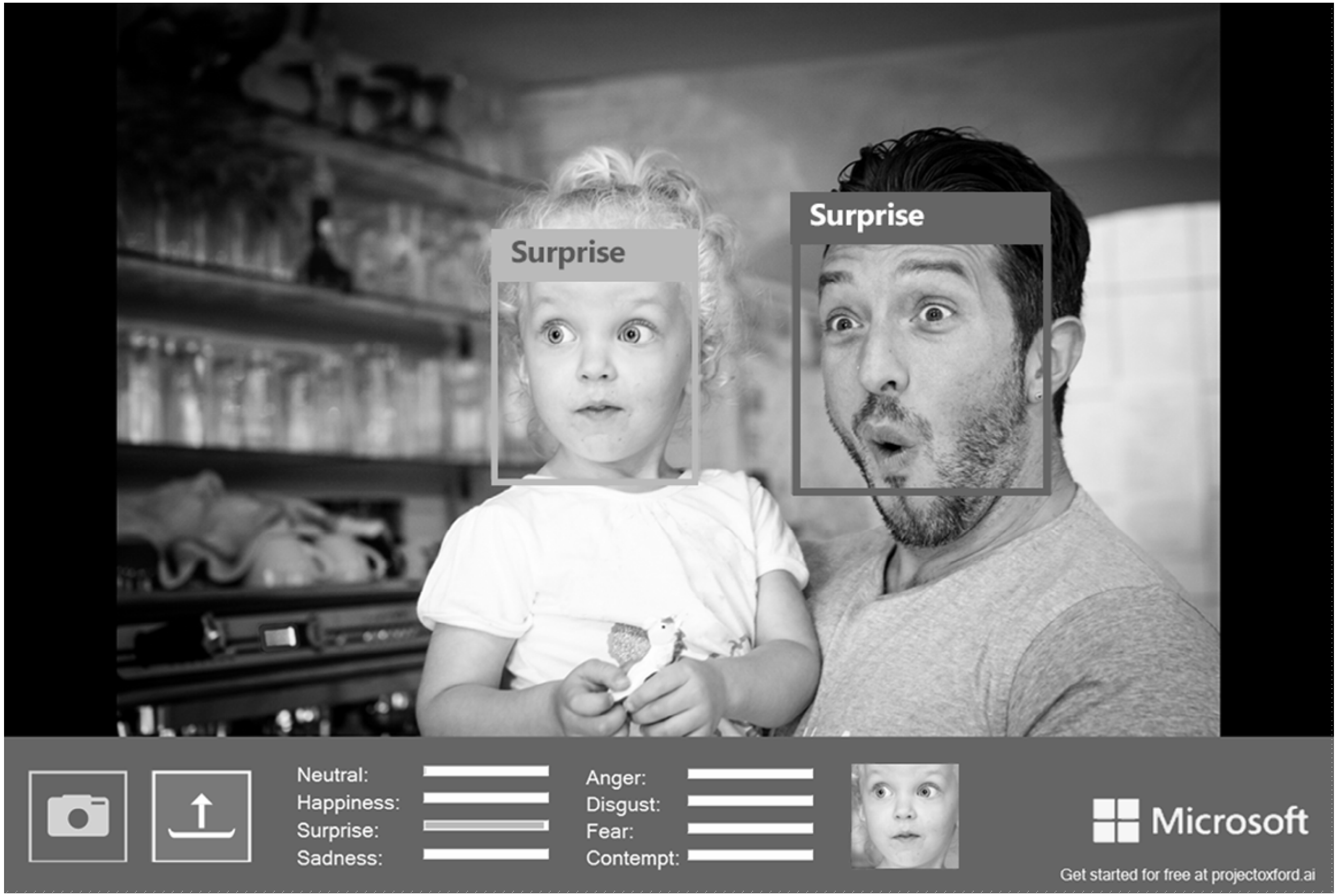
Source: NetworkWorld, Sep 20, 2014

What about predicting crime by particular individuals? Will we have predictive capabilities like those in the movie Minority Report, but through Big Data?

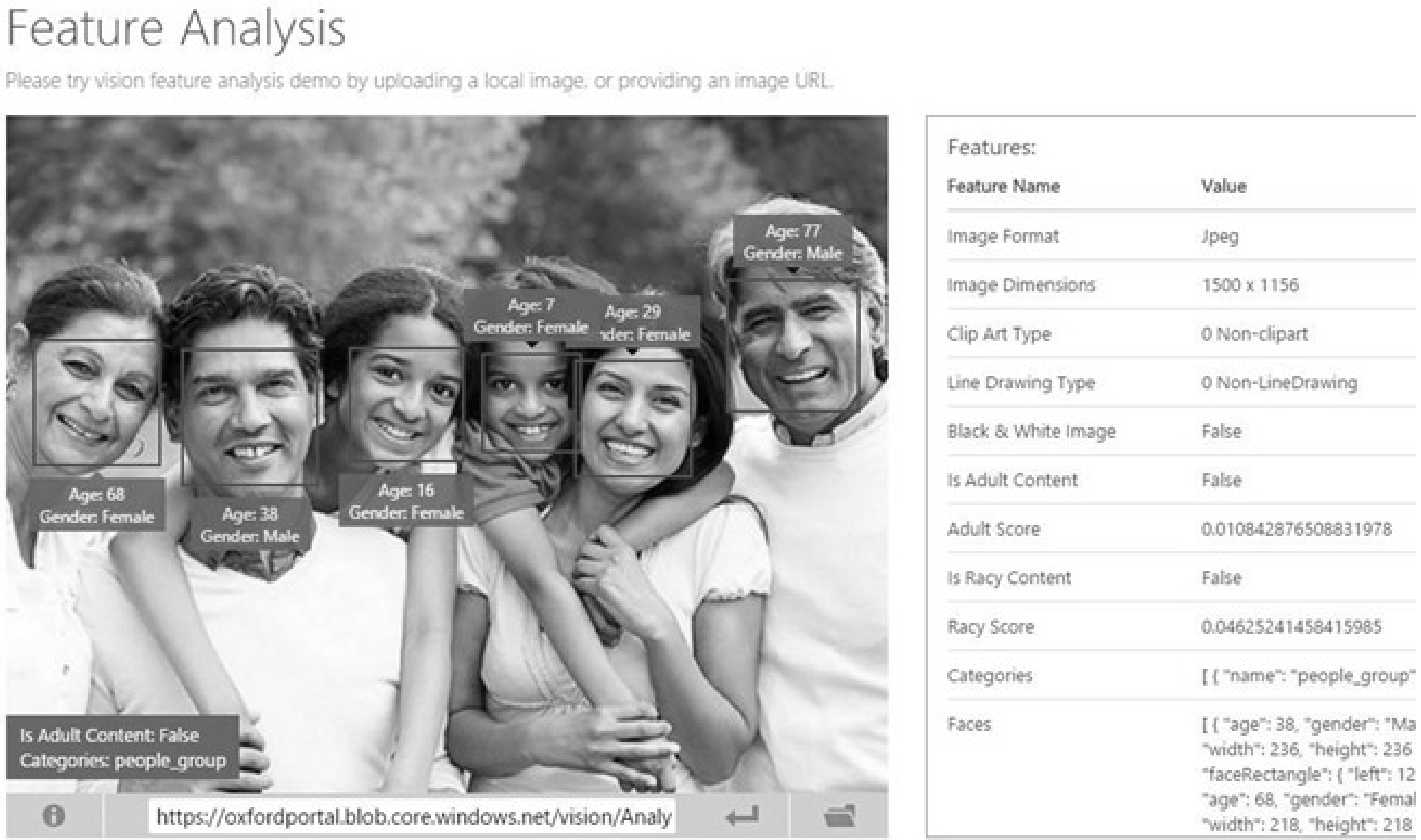
MilitaryTimes
A GANNETT COMPANY

Soldiers' suicide risk predictable with Big Data, study says, Patricia Kime, Nov. 12, 2014

Emerging Trends and Predictions
May be able to determine "Emotions"



Emerging Trends and Predictions
May be able to determine "Features"



Feature Analysis

Please try vision feature analysis demo by uploading a local image, or providing an image URL.

Is Adult Content: False
Categories: people_group

https://oxfordportal.blob.core.windows.net/vision/Analy

Features:

Feature Name	Value
Image Format	Jpeg
Image Dimensions	1500 x 1156
Clip Art Type	0 Non-clipart
Line Drawing Type	0 Non-LineDrawing
Black & White Image	False
Is Adult Content	False
Adult Score	0.010842876508831978
Is Racy Content	False
Racy Score	0.04625241458415985
Categories	[{ "name": "people_group"
Faces	[{ "age": 38, "gender": "Ma "width": 236, "height": 236 "faceRectangle": { "left": 12 "age": 68, "gender": "Femal "width": 218, "height": 218

Emerging Trends and Predictions
Helping the Blinds to “see”

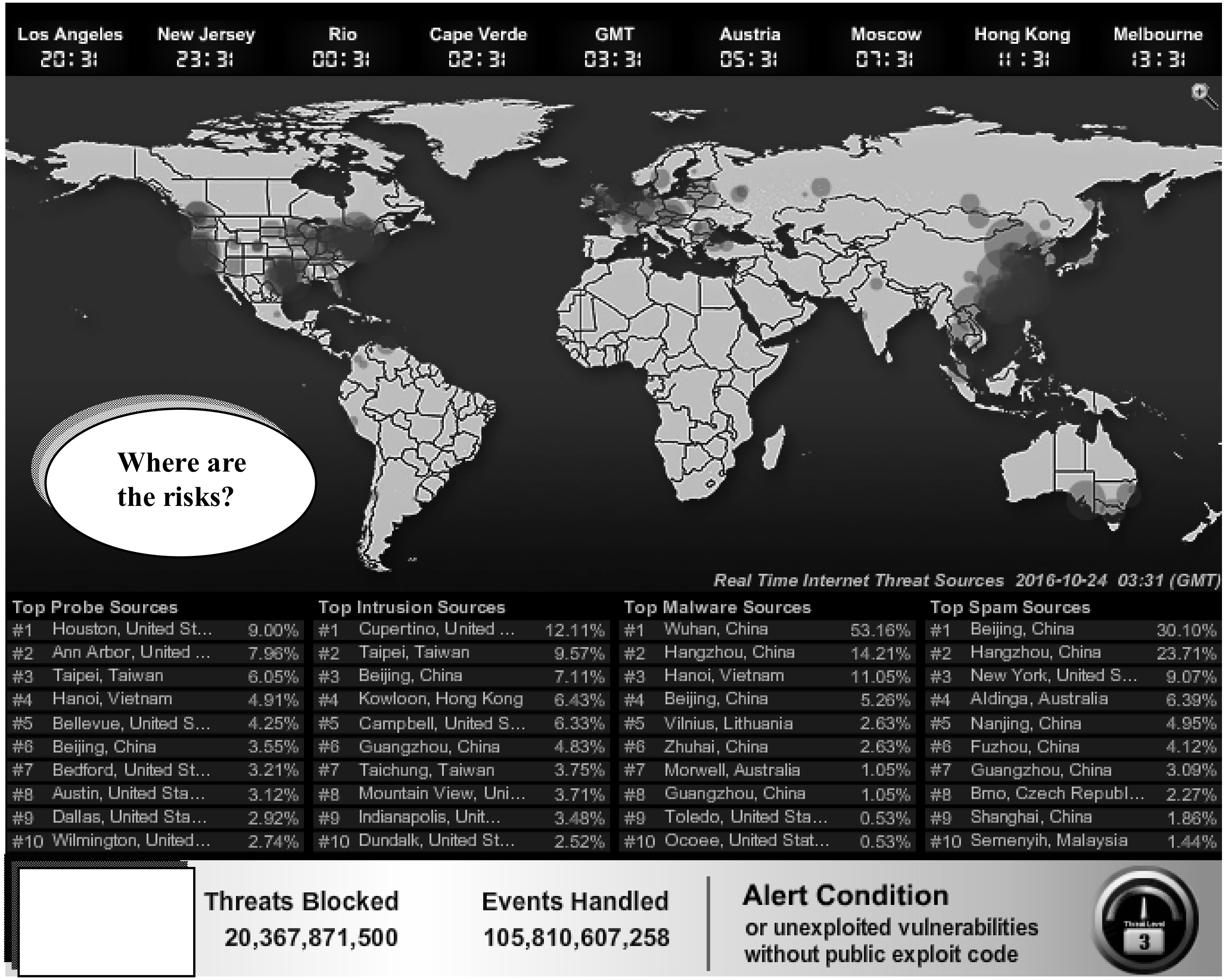
© Frank Yam 2016

Risks and Challenges

© Frank Yam 2016

Cloud Computing

Real Time Internet Threats



Los Angeles	New Jersey	Rio	Cape Verde	GMT	Austria	Moscow	Hong Kong	Melbourne
20:31	23:31	00:31	02:31	03:31	05:31	07:31	11:31	13:31

Where are the risks?

Real Time Internet Threat Sources 2016-10-24 03:31 (GMT)

Top Probe Sources		
#1	Houston, United St...	9.00%
#2	Ann Arbor, United ...	7.96%
#3	Taipei, Taiwan	6.05%
#4	Hanoi, Vietnam	4.91%
#5	Bellevue, United S...	4.25%
#6	Beijing, China	3.55%
#7	Bedford, United St...	3.21%
#8	Austin, United Sta...	3.12%
#9	Dallas, United Sta...	2.92%
#10	Wilmington, United...	2.74%

Top Intrusion Sources		
#1	Cupertino, United ...	12.11%
#2	Taipei, Taiwan	9.57%
#3	Beijing, China	7.11%
#4	Kowloon, Hong Kong	6.43%
#5	Campbell, United S...	6.33%
#6	Guangzhou, China	4.83%
#7	Taichung, Taiwan	3.75%
#8	Mountain View, Uni...	3.71%
#9	Indianapolis, Unit...	3.48%
#10	Dundalk, United St...	2.52%

Top Malware Sources		
#1	Wuhan, China	53.16%
#2	Hangzhou, China	14.21%
#3	Hanoi, Vietnam	11.05%
#4	Beijing, China	5.26%
#5	Vilnius, Lithuania	2.63%
#6	Zhuhai, China	2.63%
#7	Morwell, Australia	1.05%
#8	Guangzhou, China	1.05%
#9	Toledo, United Sta...	0.53%
#10	Ocoee, United Stat...	0.53%

Top Spam Sources		
#1	Beijing, China	30.10%
#2	Hangzhou, China	23.71%
#3	New York, United S...	9.07%
#4	Aldinga, Australia	6.39%
#5	Nanjing, China	4.95%
#6	Fuzhou, China	4.12%
#7	Guangzhou, China	3.09%
#8	Brno, Czech Republ...	2.27%
#9	Shanghai, China	1.86%
#10	Semenyih, Malaysia	1.44%

Threats Blocked 20,367,871,500

Events Handled 105,810,607,258

Alert Condition
or unexploited vulnerabilities
without public exploit code

© Frank Yam 2016

Risks and Security Concerns

Service and contractual risks

Vendor Lock In	▪ Few tools, procedures or standard formats available for data and service portability
Poor SLA	▪ Service level affects confidentiality and availability
3rd Party access to Data	▪ The needs to protect the intellectual property, trade secrets; and complied to regulations and laws in different geographical regions
Poor DR Plan	▪ Business continuity and disaster recovery plans must be well documented and tested

© Frank Yam 2016

Risks and Security Concerns

Technology risks

Integration / Bandwidth

- How to integrate the in-house systems to the Cloud ?
- High speed bandwidth ready ?

Encryption and Key Mgnt

- Speedy encryption / decryption;
- Key management

Testing and Monitoring

- Provider may not allow you to do thorough PEN test, audit;
- Are there good monitoring tools available ?

Resource Allocation

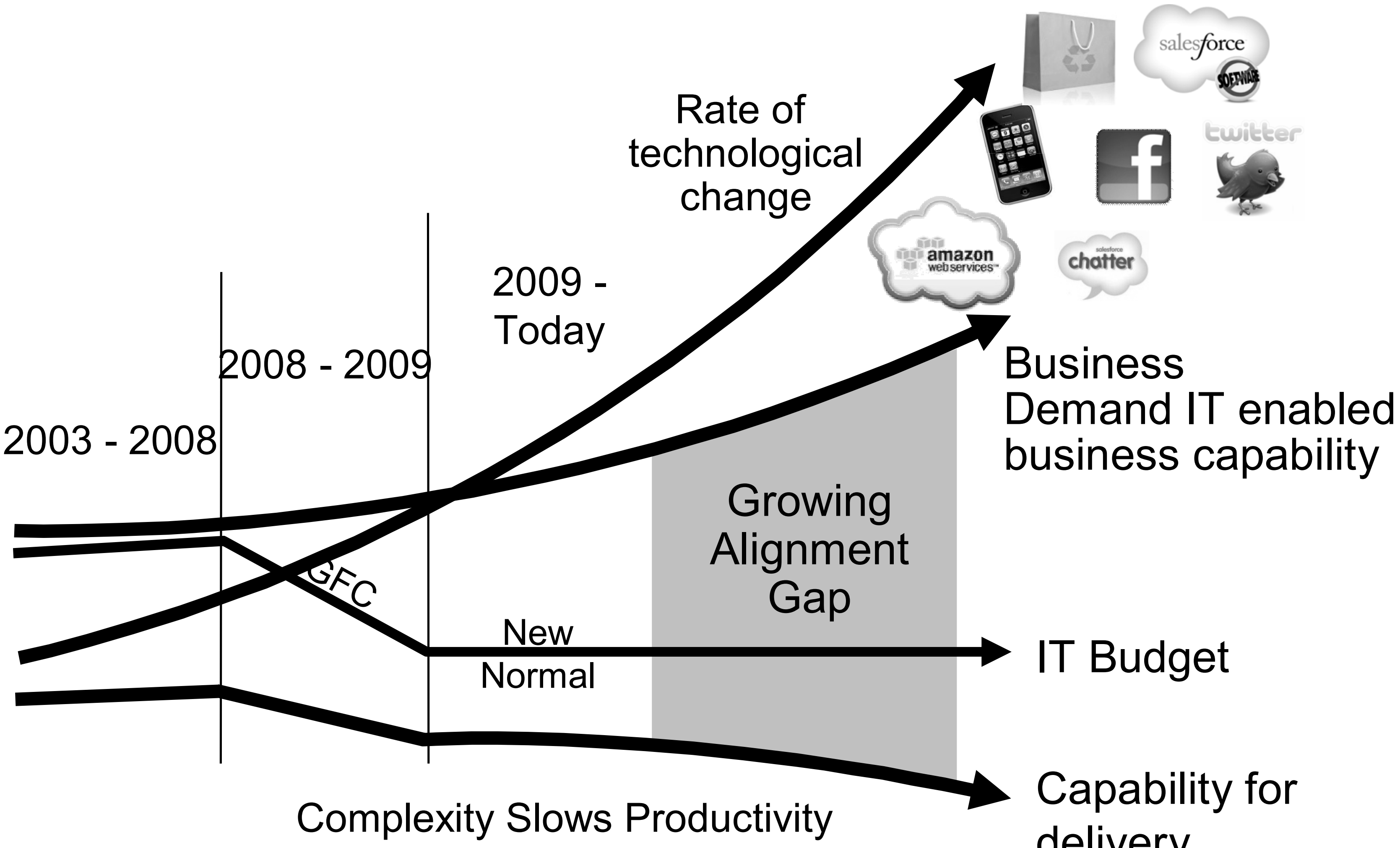
- Overbooking, underbooking;
- Handling of DOS attack; Payment cap

Applicability for Cloud Computing

Source: Federal Reserve System, USA

System Type	Scalability	Availability	Security	
Information site	**Medium**	**Medium**	**Low**	**Public /Hybrid**
External Collaboration	**Medium**	**Medium**	**Medium**	**Public /Hybrid**
Public research / survey	**Low**	**Medium**	**Medium**	**Public /Hybrid**
Internal R&D	**Low**	**Low**	**Medium**	**Public /Hybrid**
Disaster Recovery	**Medium**	**Medium**	**Medium**	**Public /Hybrid**
Application Test and QA	**Low**	**Medium**	**Medium**	**Private**
Application Development	**Low**	**Medium**	**Medium**	**Private**
Production Applications	**High**	**High**	**Medium**	**No**
Mission Critical Applications	**High**	**High**	**High**	**No**

Growing Alignment Gap



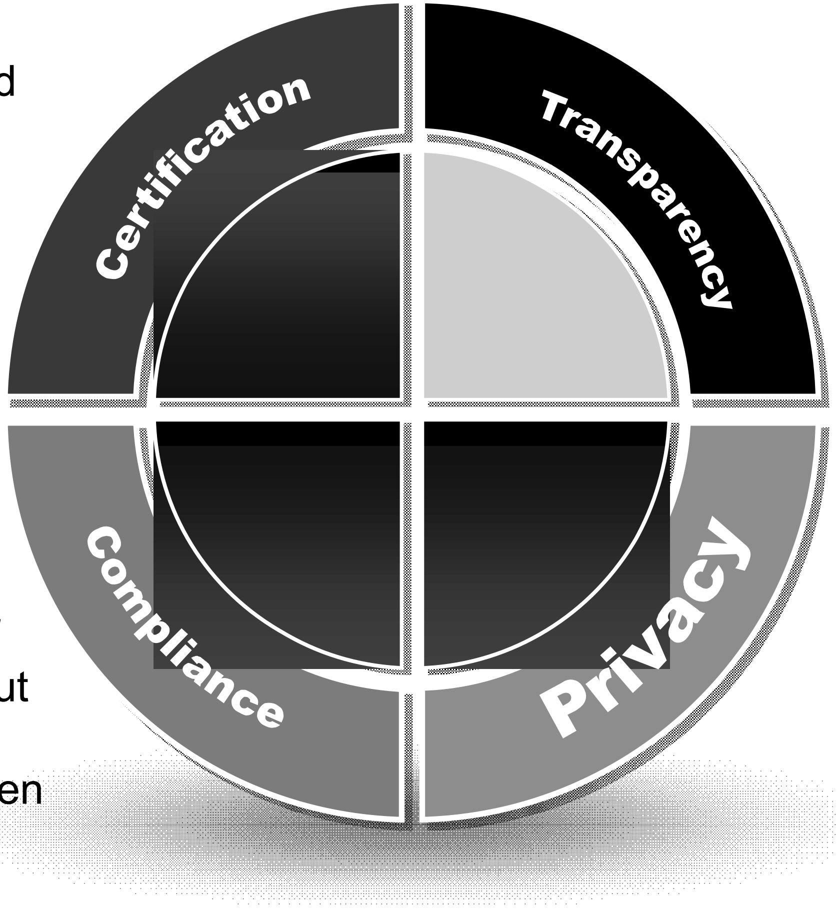
50-80% of budget spent keeping lights on

© Frank Yam 2016

Audit and Control

Assurance Considerations

Independent assurance from third-party audits and service auditor reports



Must demonstrate existence of effective and robust security controls

Ensure the compliance of various countries' laws, but at the same time able to access your own data when needed

Must prove that privacy controls are in place and able to prevent, detect and react to breaches

© Frank Yam 2016

ISACA

1995	NOW
EDPAA	ISACA
IT auditors…	… and risk managers, privacy officers, compliance professionals, information security experts, IT control and IT governance professionals **(+ cybersecurity professionals)**
CISA…	… and CISM, CGEIT and CRISC **(+ CSX I, II, III)**
COBIT	**COBIT 5** and **COBIT Online**
～9,000 members	Now serving over 140,000 professionals

© Frank Yam 2016

ISACA's Vision and Mission

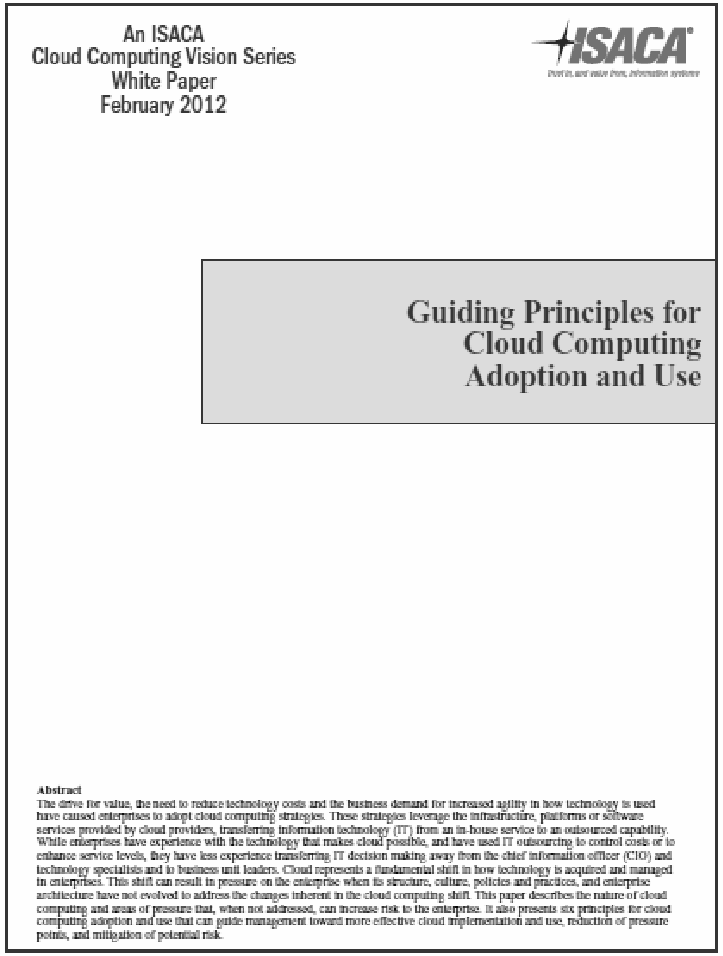
ISACA's vision *(to aspire to as an organization)*

"Trust in, and value from, information systems"

ISACA's mission *(to guide decision making and investments)*

41

ISACA's Six Guiding Principles for Adopting and Using the Cloud



An ISACA
Cloud Computing Vision Series
White Paper
February 2012

Guiding Principles for Cloud Computing Adoption and Use

Abstract

The drive for value, the need to reduce technology costs and the business demand for increased agility in how technology is used have caused enterprises to adopt cloud computing strategies. These strategies leverage the infrastructure, platforms or software services provided by cloud providers, transferring information technology (IT) from an in-house service to an outsourced capability. While enterprises have experience with the technology that makes cloud possible, and have used IT outsourcing to control costs or to enhance service levels, they have less experience transferring IT decision making away from the chief information officer (CIO) and technology specialists and to business unit leaders. Cloud represents a fundamental shift in how technology is acquired and managed in enterprises. This shift can result in pressure on the enterprise when its structure, culture, policies and practices, and enterprise architecture have not evolved to address the changes inherent in the cloud computing shift. This paper describes the nature of cloud computing and areas of pressure that, when not addressed, can increase risk to the enterprise. It also presents six principles for cloud computing adoption and use that can guide management toward more effective cloud implementation and use, reduction of pressure points, and mitigation of potential risk.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

- Enablement
- Cost benefit
- Enterprise risk
- Capability
- Accountability
- Trust

Additional Resources

ISACA®

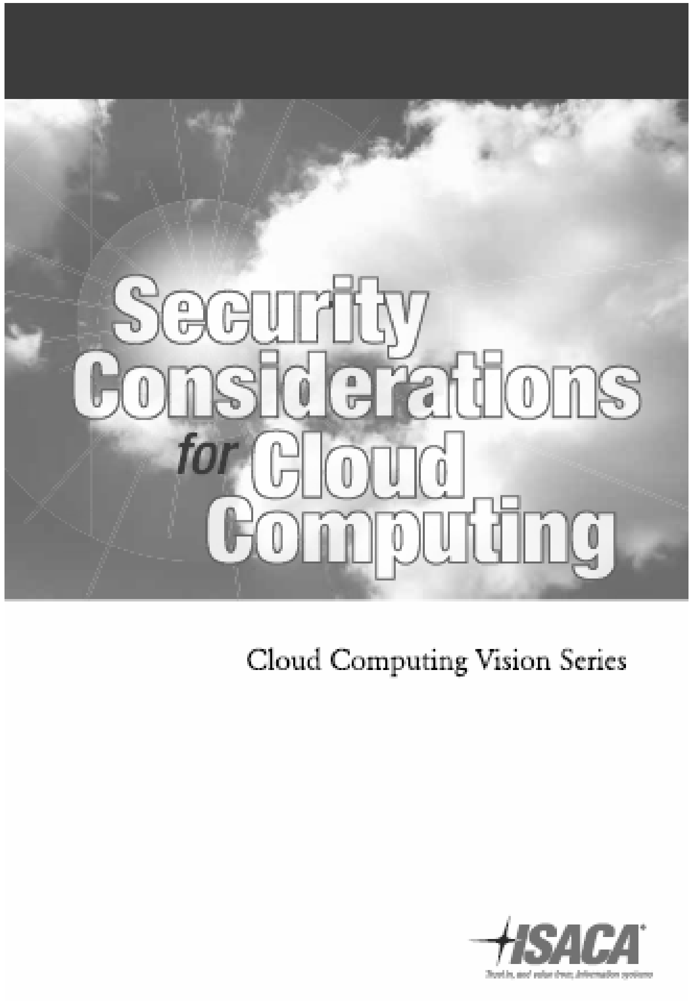
Trust in, and value from, information systems

COBIT® 5

AN ISACA® FRAMEWORK

CONTROLS AND ASSURANCE IN THE CLOUD:

Using COBIT® 5



Security Considerations for Cloud Computing

Cloud Computing Vision Series

ISACA®

Trust in, and value from, information systems

FOCUS

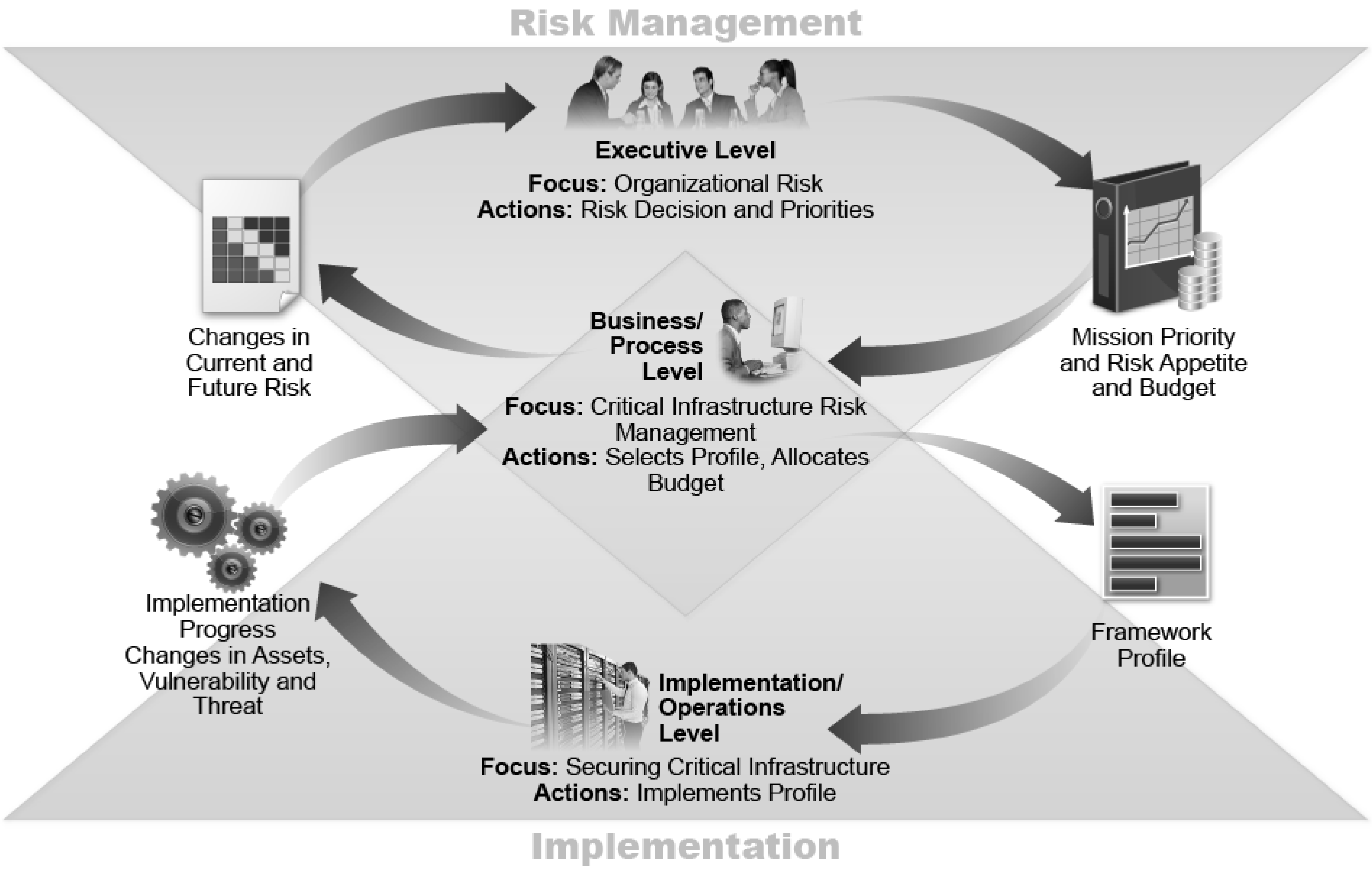
Cybersecurity

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Cybersecurity Framework

NIST Cybersecurity Framework

Information and Decision Flows within an Organization



Risk Management

Executive Level

Focus: Organizational Risk
Actions: Risk Decision and Priorities

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

Business/ Process Level

Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget

Implementation Progress
Changes in Assets, Vulnerability and Threat

Framework Profile

Implementation/ Operations Level

Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

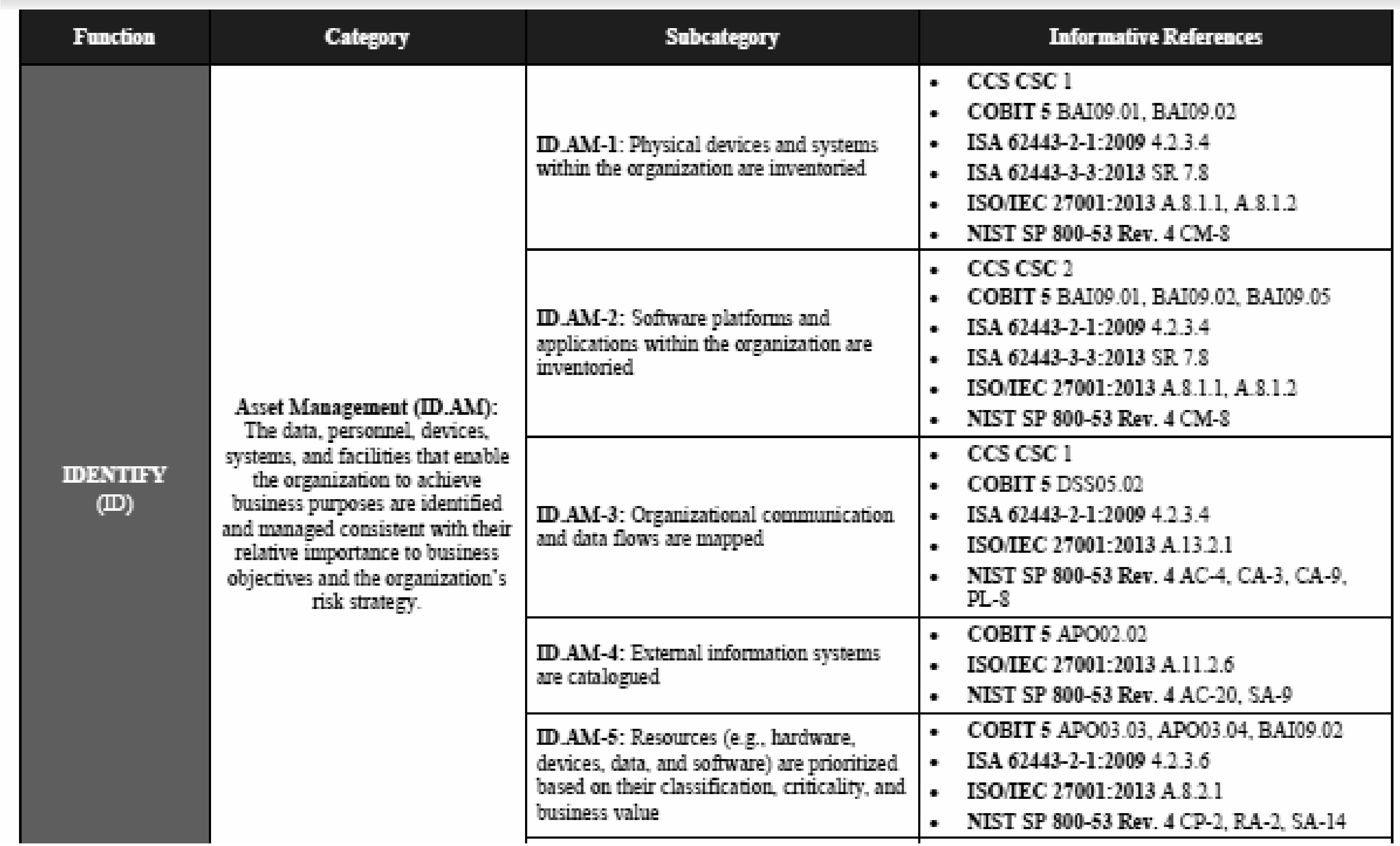
Source: NIST Cybersecurity Framework

© Frank Yam 2016

NIST Cybersecurity Framework

Function	Categories
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Assessment Strategy
Protect	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

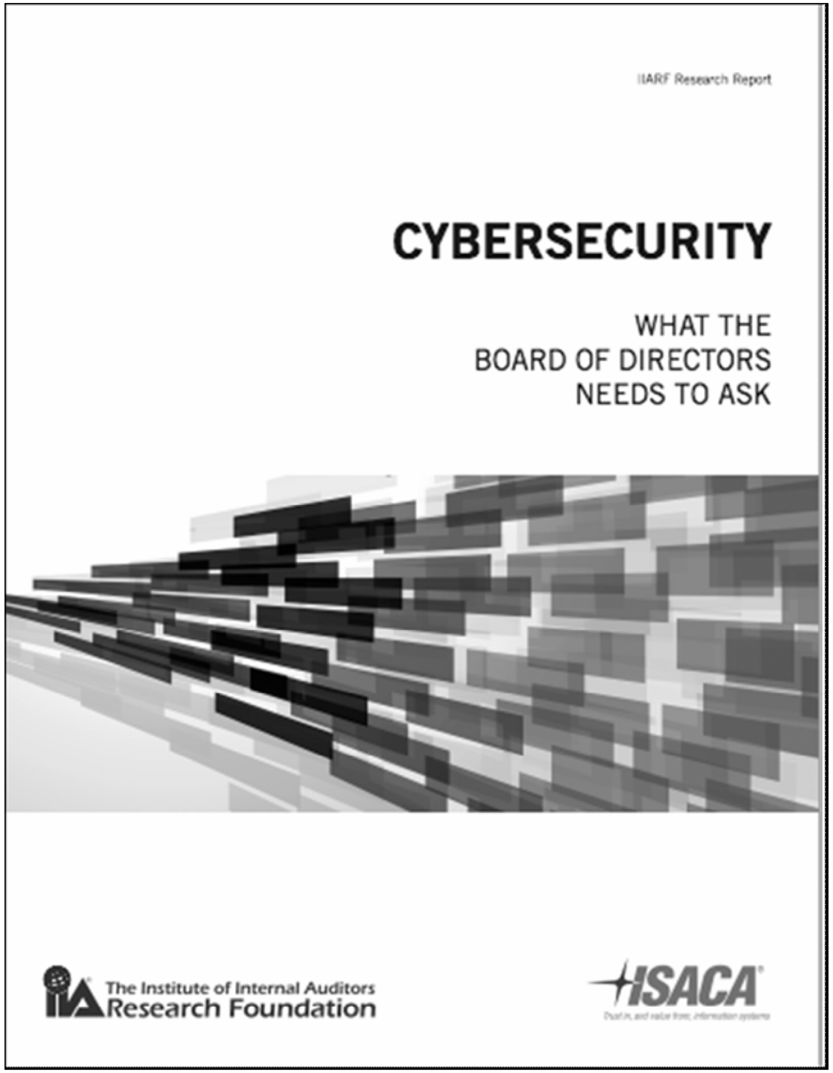
NIST Cybersecurity Framework



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	- **CCS CSC 1** - **COBIT 5** BAI09.01, BAI09.02 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISA 62443-3-3:2013** SR 7.8 - **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 - **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	- **CCS CSC 2** - **COBIT 5** BAI09.01, BAI09.02, BAI09.05 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISA 62443-3-3:2013** SR 7.8 - **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 - **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	- **CCS CSC 1** - **COBIT 5** DSS05.02 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISO/IEC 27001:2013** A.13.2.1 - **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	- **COBIT 5** APO02.02 - **ISO/IEC 27001:2013** A.11.2.6 - **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	- **COBIT 5** APO03.03, APO03.04, BAI09.02 - **ISA 62443-2-1:2009** 4.2.3.6 - **ISO/IEC 27001:2013** A.8.2.1 - **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14

© Frank Yam 2016

ISACA Publications on Cybersecurity



IIARF Research Report

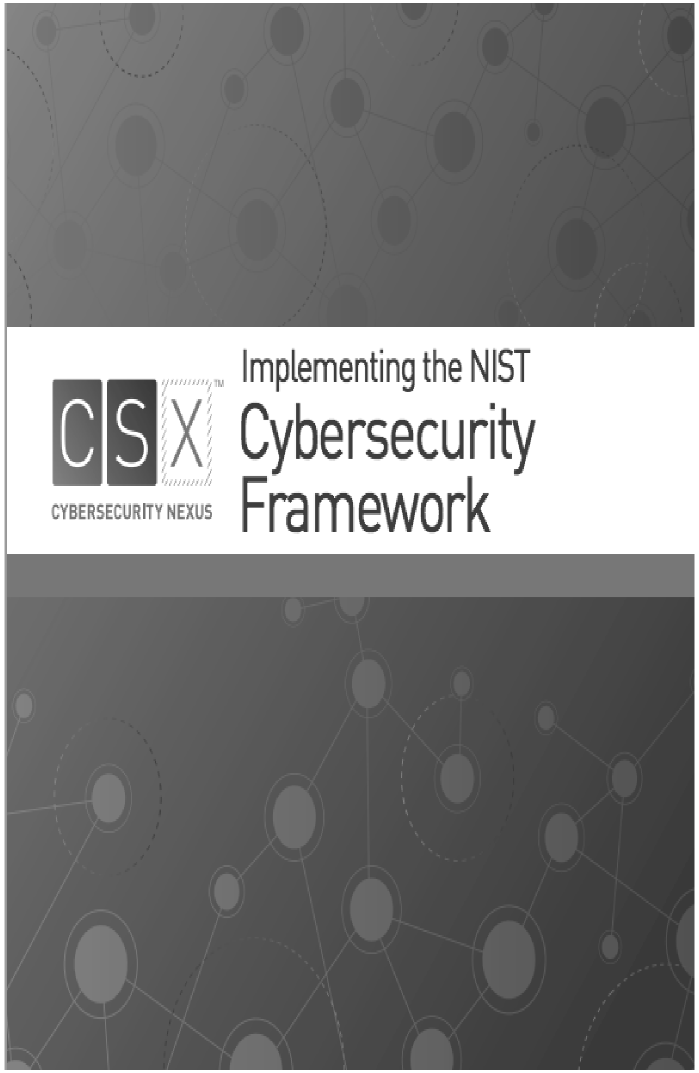
CYBERSECURITY

WHAT THE
BOARD OF DIRECTORS
NEEDS TO ASK

The Institute of Internal Auditors
Research Foundation

ISACA®

Trust in, and value from, information systems



CSX™
CYBERSECURITY NEXUS

Implementing the NIST
Cybersecurity
Framework

NEW CYBERSECURITY CERTIFICATIONS

CSX P
Certified Cybersecurity Practitioner

CSX Practitioner —Demonstrates ability to serve as a first responder to a cybersecurity incident following established procedures and defined processes. (1 certification, 3 training courses; prerequisite for CSX Specialist)

CSX S
Certified Cybersecurity Specialist

CSX Specialist —Demonstrates effective skills and deep knowledge in one or more of the five areas based closely on the NIST Cybersecurity Framework: Identify, Detect, Protect, Respond and Recover. (**5 certifications**, 5 training courses; requires CSX Practitioner)

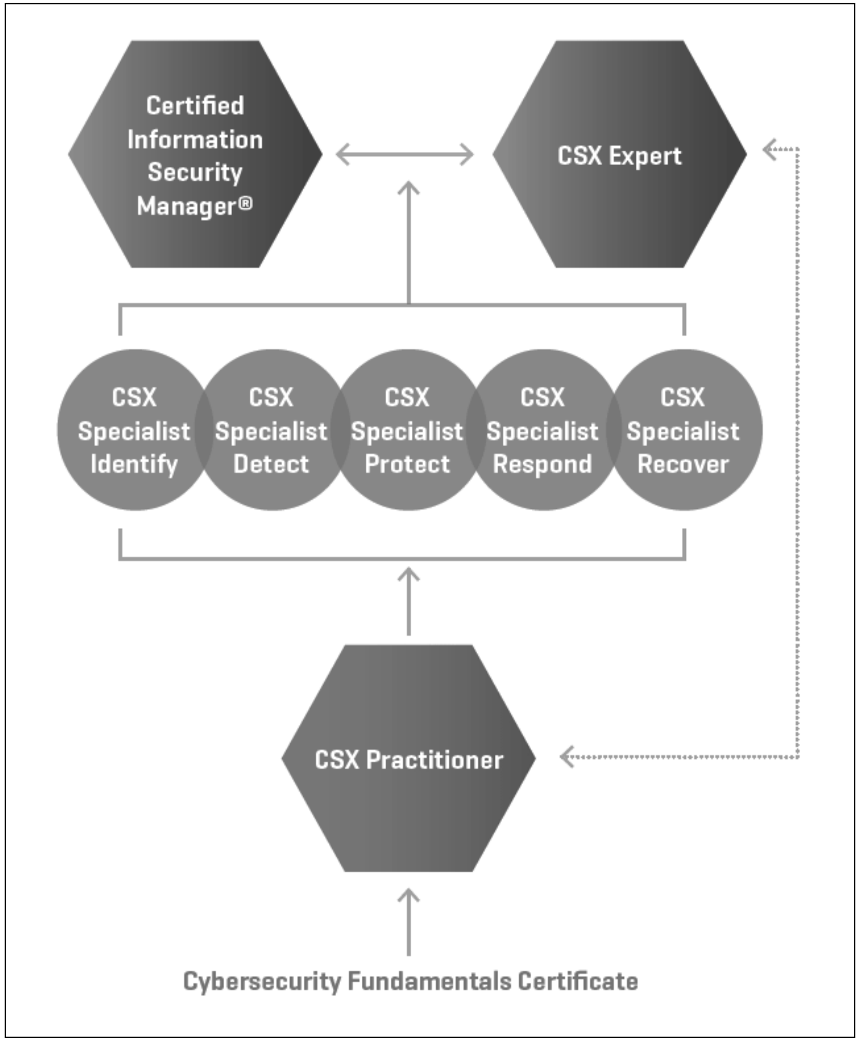
CSX E
Certified Cybersecurity Expert

CSX Expert —Demonstrates ability of a master/expert-level cybersecurity professional who can identify, analyze, respond to, and mitigate complex cy ; no prerequisites re

NEW CYBERSECURITY CERTIFICATIONS

CSX
CERTIFICATIONS

CSX training and certifications offered for skill levels and specialties throughout a professional's career.



Certified Information Security Manager®

CSX Expert

CSX Specialist Identify

CSX Specialist Detect

CSX Specialist Protect

CSX Specialist Respond

CSX Specialist Recover

CSX Practitioner

Cybersecurity Fundamentals Certificate

www.isaca.org/csx-certifications

Where can I find Good Sources for Reference?

- HKCERT (Hong Kong Computer Emergency Response Team Coordination Centre)
  - www.hkcert.org
- HKSAR InfoSec Website
  - www.infosec.gov.hk
- ISACA
  - www.isaca.org/cyber

What are some of the common tools being used in practice?

- Data Analytics Software (e.g. ACL、IDEA、Excel)
- Network Mapping Software（e.g. Nmap)
- Forensics Software (e.g. EnCase， FTK， X-ways）
- eDiscovery Software (e.g. Nuix, Relativity)

© Frank Yam 2016

Seminar Summary

© Frank Yam 2016

Key Messages

- Organisations (and individuals) will rely more and more on Cloud Computing
- We should anticipate more Cloud-related risks (and frauds)
- We will be expected to understand Cloud-related risks and to recommend appropriate controls
- Focus on People
- One can be influenced by other’s behavior (i.e. benchmarks, norms, industry practices)

© Frank Yam 2016

Let’s play our parts !

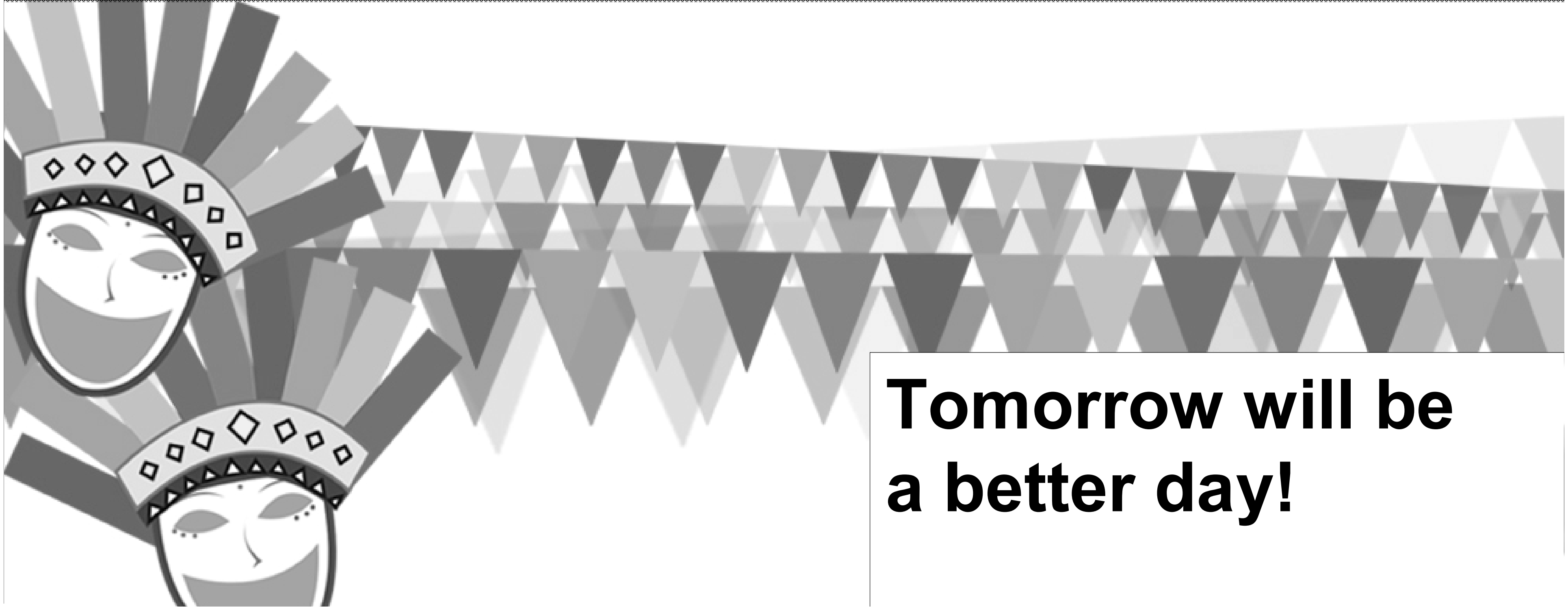
We need to work together and help each other

to

SURVIVE!

© Frank Yam 2016

56



Tomorrow will be
a better day!