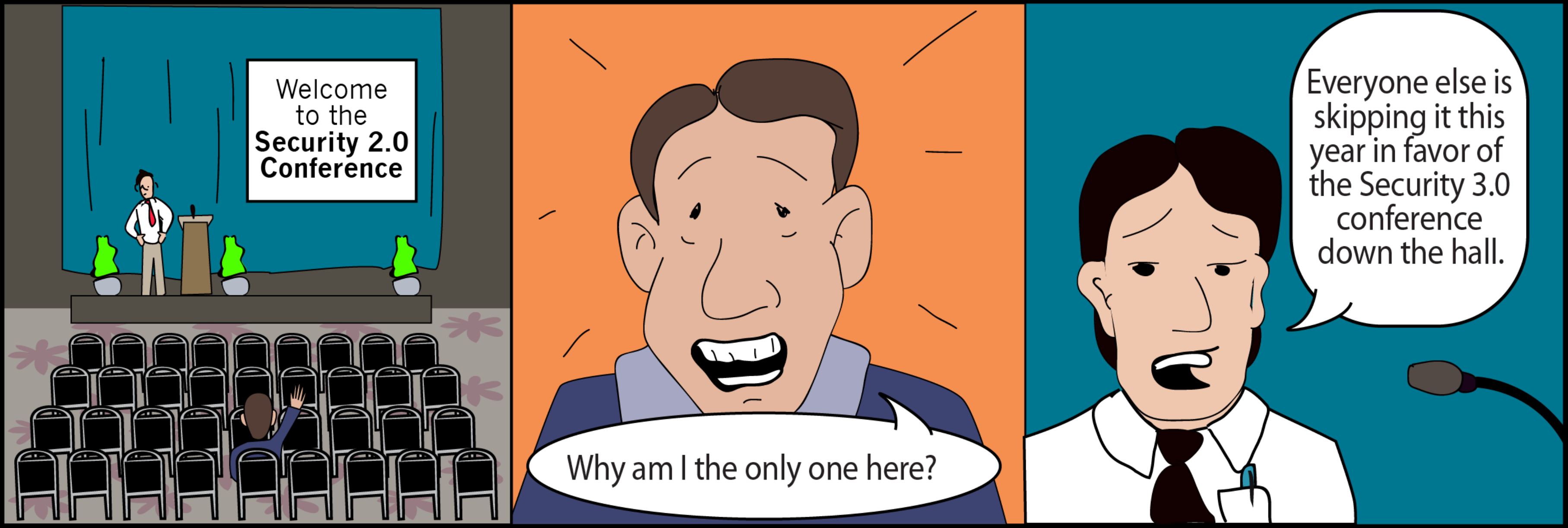
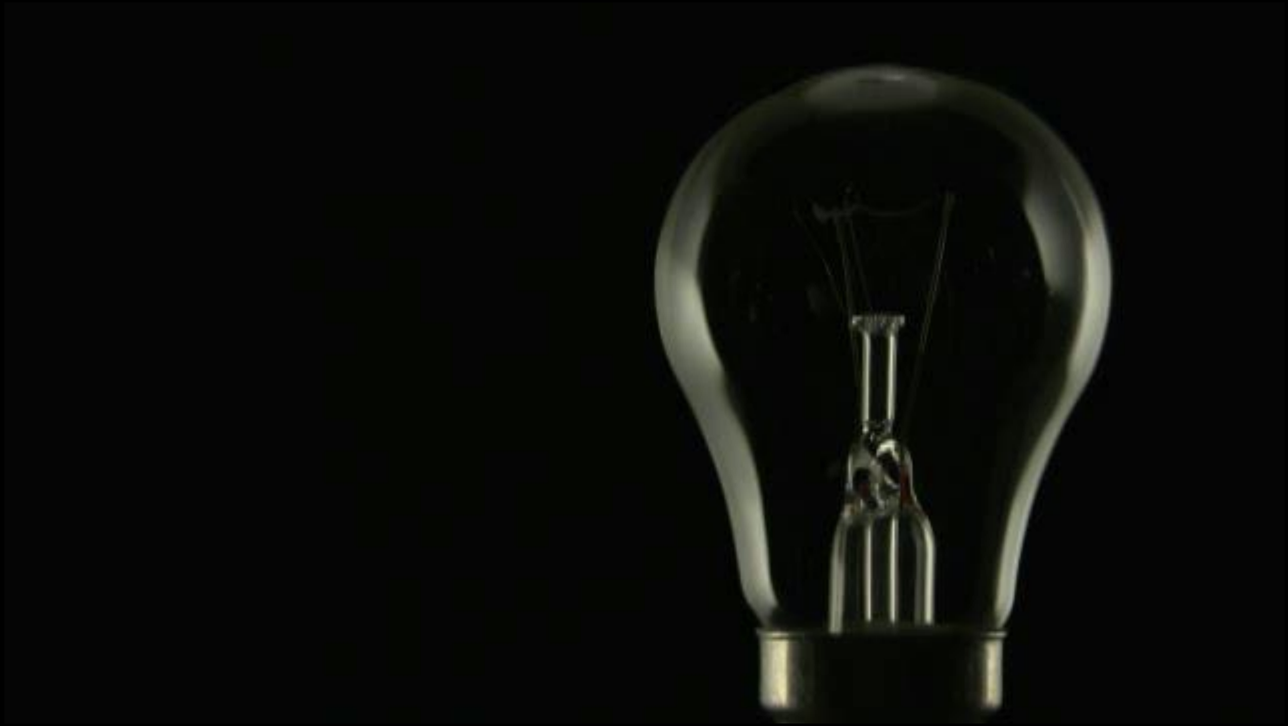

Welcome to the Security 2.0 Conference
Why am I the only one here?
Everyone else is skipping it this year in favor of the Security 3.0 conference down the hall.

"It's difficult to get a man to understand something when his salary depends on him not understanding it"

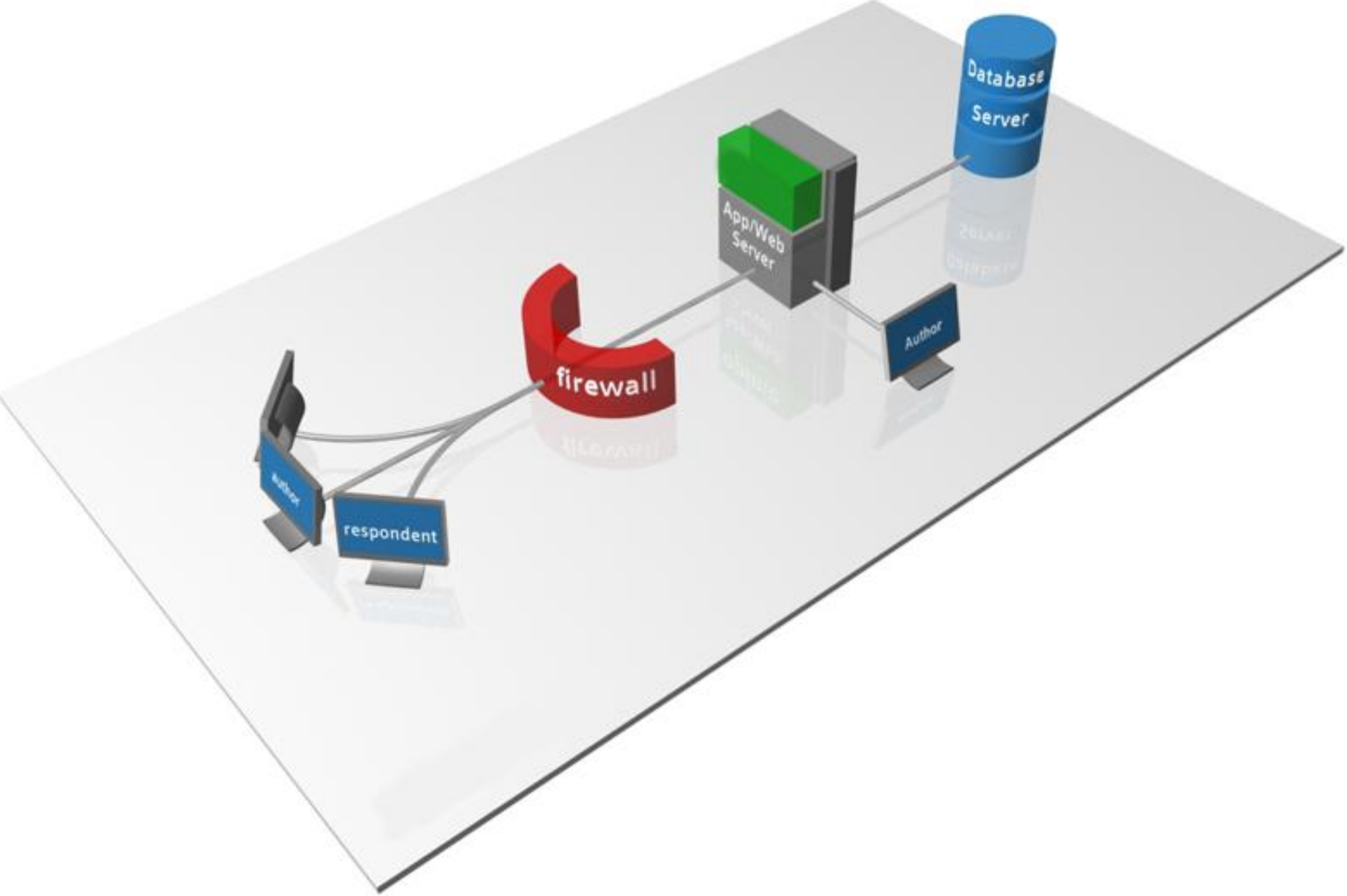
- Upton Sinclair (spoken by Al Gore)

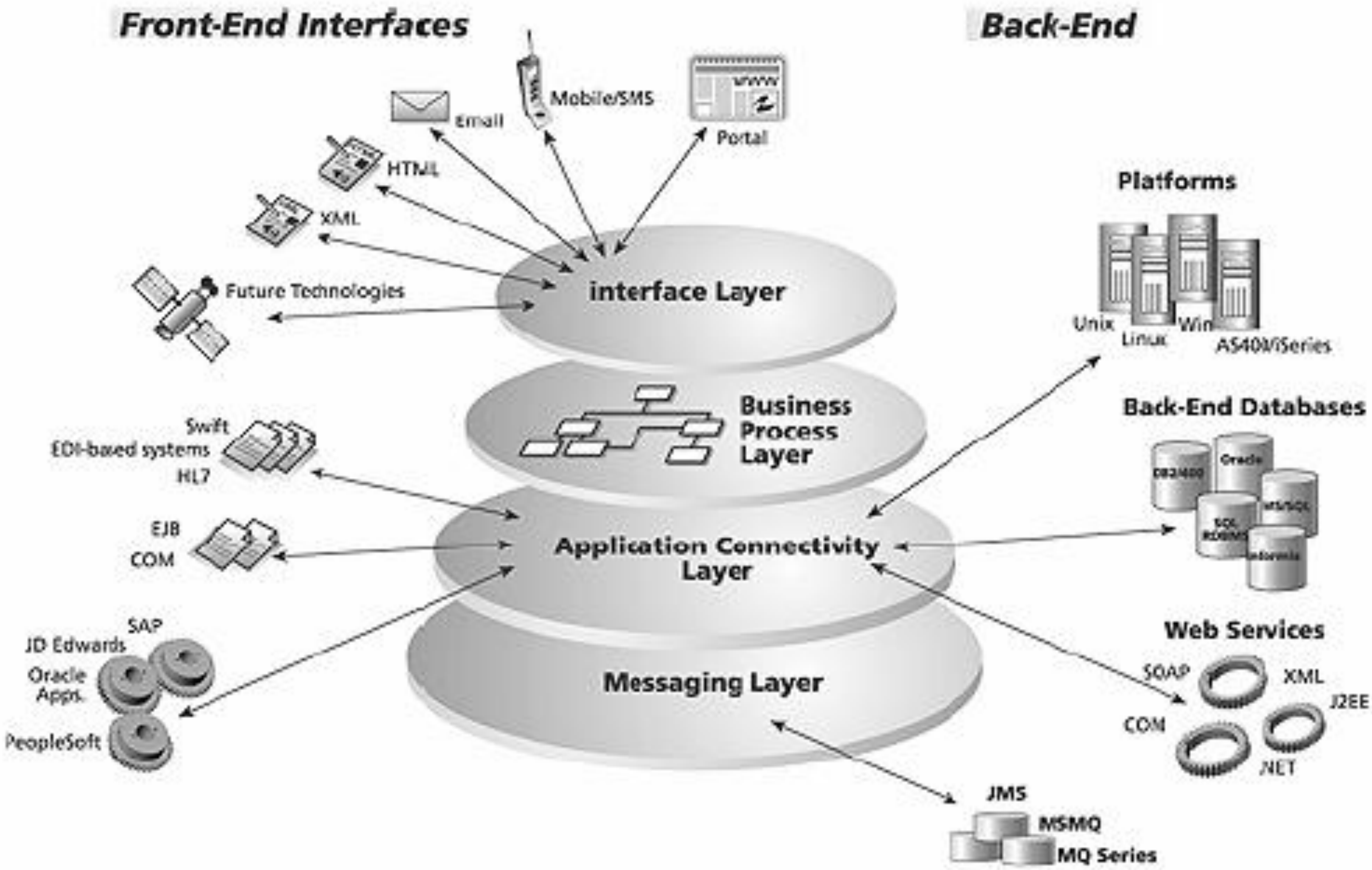
Agenda

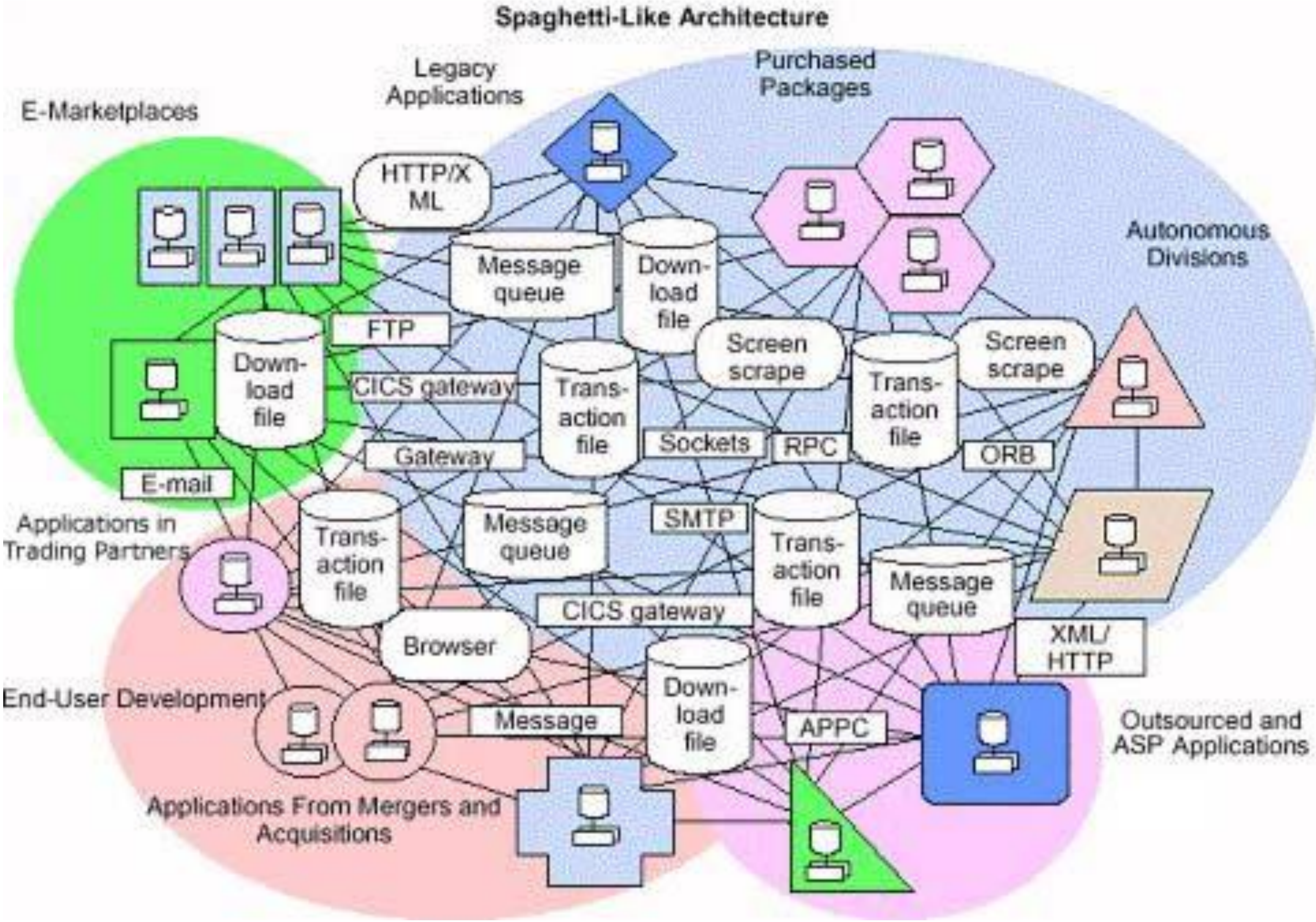
- My OWASP Story and the Importance of Application Security Today
- Inconvenient Security Truths
  - Complexity
  - Context
  - Compliance FUD
  - Understanding the Real Problem
  - The Security Gold Rush
  - Ground Hog Day
  - Super Heros
  - Fools and Tools
- Interesting Things to Look Out for Tomorrow
  - Super Crunching
  - The World is Flat
  - Crowd Sourcing
  - Checklists Aren’t For Dummies



Complexity


Database Server
App/Web Server
Author
firewall
author
respondent


Front-End Interfaces
Back-End
Mobile/SMS
Email
Portal
HTML
XML
Future Technologies
interface Layer
Platforms
Unix
Linux
Win
AS400/iSeries
Business
Process
Layer
Swift
EDI-based systems
HL7
Back-End Databases
DB2/400
Oracle
MS/SQL
SQL
RDBMS
Informix
EJB
COM
Application Connectivity
Layer
Web Services
SAP
JD Edwards
Oracle
Apps.
PeopleSoft
Messaging Layer
SOAP
XML
J2EE
COM
.NET
JMS
MSMQ
MQ Series


Spaghetti-Like Architecture
Legacy Applications
Purchased Packages
E-Marketplaces
HTTP/XML
Message queue
Down-load file
Autonomous Divisions
FTP
Screen scrape
Screen scrape
Down-load file
CICS gateway
Trans-action file
Trans-action file
Sockets
RPC
ORB
Gateway
E-mail
SMTP
Applications in Trading Partners
Trans-action file
Message queue
Trans-action file
Message queue
CICS gateway
XML/HTTP
Browser
Down-load file
End-User Development
Message
APPC
Outsourced and ASP Applications
Applications From Mergers and Acquisitions

Context

Compliance FUD

3 Types of Compliance

1. Government Regulations
2. Industry Standards
3. Marketing FUD

REMEMBER: YOU CAN'T SPELL COMPLIANCE WITHOUT 'LIANCE'

“If You Think Technology Is the Solution, You Don’t Understand the Problem”

- Bruce Schneier

“If you fail a penetration test you know you have a problem, if you pass a penetration test you don’t know you don’t have a problem”.

- Gary McGraw

“You need ~~PKI~~, ~~WAF~~, ~~GRC~~.....to cure all your wrongs”

“In the future everyone will have their 15 minutes of fame” – Andy Warhol

CALIFORNIA GOLD RUSH 1849
GOLD RUSH
USA
33
1999

A fool with a tool …. is still a fool

(British Slang Version: A tool with a tool …. is definitely a tool)

News for people who run tools

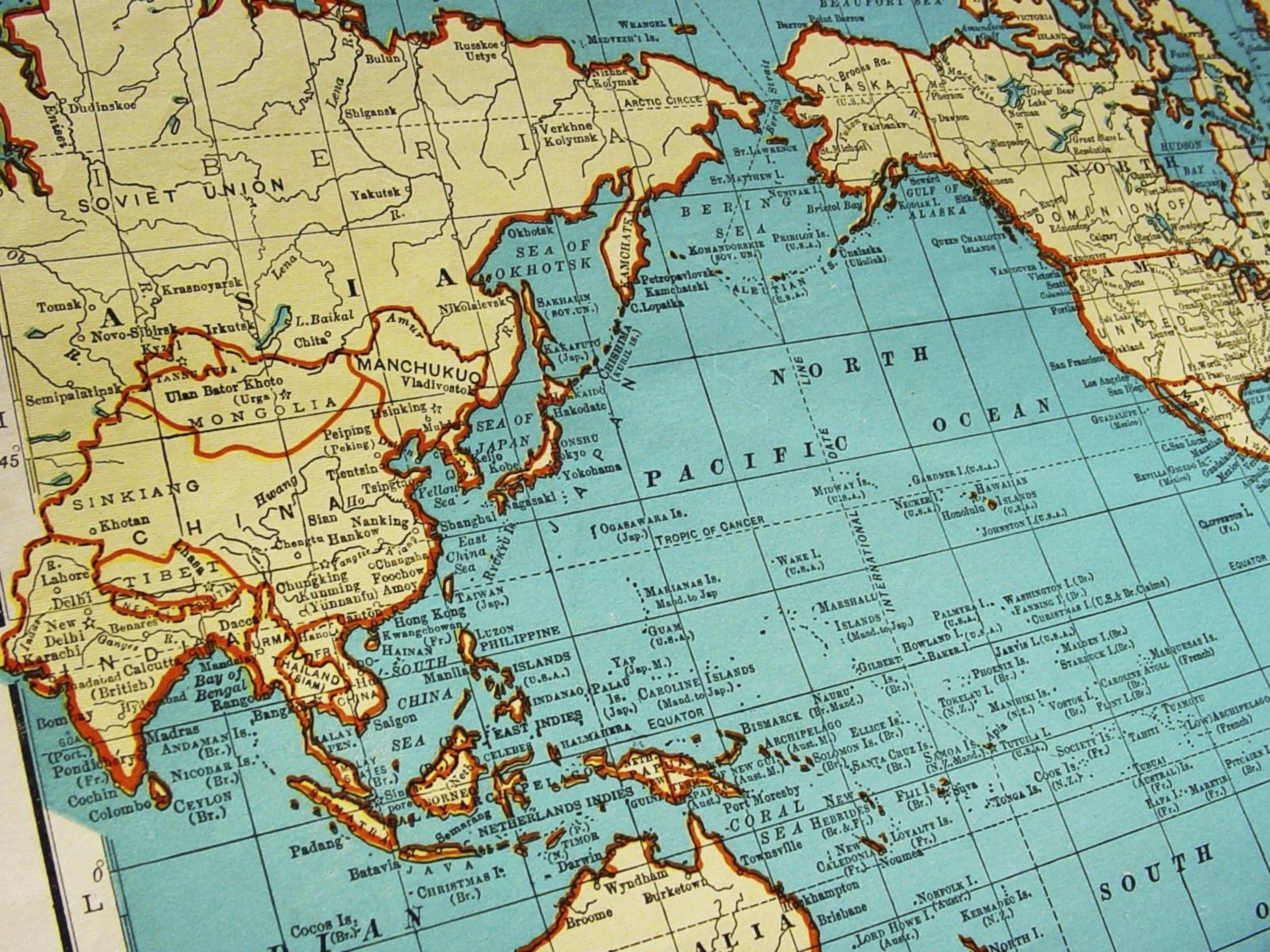
China!

China!

China!

China!

Wine Quality = 12.145 + 0.00117 Winter Rainfall + 0.0614 Average Growing Season Temperature - 0.00386 Harvest Rainfall


BEAUFORT SEA
WRANGEL I.
MEDVEZH'I Is.
Barrow
Point Barrow
VICTORIA
ISLAND
Russkoe Ustye
Bulun
Lena
R.
Dudinskoe
Enisei
Shigansk
Nizhne Kolymsk
ARCTIC CIRCLE
Bering Strait
Brooks Ra.
ALASKA
(U.S.A.)
Yukon
Fairbanks
Nome
St. Michael
Dawson
Great Bear Lake
Norman
Great Slave L.
Resolution
Simpson
HUDSON
BAY
Verkhne Kolymsk
S I B E R I A
SOVIET UNION
Yakutsk
R.
ST. LAWRENCE I.
ST. MATTHEW I.
NUNIVAK I.
Bristol Bay
Cordova
Seward
GULF OF ALASKA
KODIAK I.
Sitka
NORTH
DOMINION OF CANADA
Prince Rupert
Edmonton
Calgary
Regina
Winnipeg
BERING SEA
PRIBILOF Is. (U.S.A.)
KOMANDORSKIE (SOV. UN.)
Unalaska (Ulliuliuk)
ALEUTIAN IS. (U.S.A.)
QUEEN CHARLOTTE ISLANDS
VANCOUVER I.
Victoria
Seattle
Columbia
Portland
Butte
AMERICA
UNITED STATES
Salt Lake City
Denver
Kansas City
Oakland
San Francisco
Los Angeles
San Diego
Ft. Worth
El Paso
Houston
Okhotsk
SEA OF OKHOTSK
KAMCHATKA
Petropavlovsk Kamchatski
C. Lopatka
Ob
Tomsk
Krasnoyarsk
A S I A
Novo-Sibirsk
Irkutsk
L. Baikal
Chita
Amur
Nikolaievsk
SAKHALIN (SOV. UN.)
KARAFUTO (Jap.)
CHISHIMA (KURIL Is.)
Kyzyl
TANNU TUVA
Ulan Bator Khoto (Urga)
MONGOLIA
Semipalatinsk
MANCHUKUO
Vladivostok
Hsinking
Mukden
HOKKAIDO
Hakodate
SEA OF JAPAN
HONSHU
Tokyo
Yokohama
Kobe
Keijo
CHOSEN
Nagasaki
J A P A N
NORTH
PACIFIC
OCEAN
DATE LINE
INTERNATIONAL
Peiping (Peking)
Tientsin
Tsingtao
Yellow Sea
Hwang
Ho
SINKIANG
Khotan
C H I N A
Sian
Nanking
Hankow
Shanghai
Chengtu
Yangtze Kiang
Changsha
East China Sea
RYUKYU Is.
Lhasa
TIBET
Lahore
Delhi
New Delhi
Benares
Ganges R.
NEPAL
BHUTAN
Dacca
Chungking
Kunming (Yünnanfu)
Foochow
Amoy
TAIWAN (Jap.)
Canton
Hong Kong
Kwangchowan (Fr.)
HAINAN
Hanoi
BURMA
Mandalay
Rangoon
THAILAND (SIAM)
FR. INDO-CHINA
Hue
Bangkok
Saigon
Indus
Karachi
I N D I A
Calcutta
(British)
Hyderabad
Bay of Bengal
Bombay
GOA (Port.)
Madras
Pondichery (Fr.)
Cochin
Colombo
CEYLON (Br.)
ANDAMAN Is. (Br.)
NICOBAR Is. (Br.)
SOUTH CHINA SEA
MALAY PEN.
MALAY STATES (Br.)
Singapore
SUMATRA
Padang
Batavia
JAVA
Semarang
BORNEO
Neth.
CELEBES
NETHERLANDS INDIES
EAST INDIES
HALMAHERA
ARCHIPELAGO
TIMOR
Darwin
(P.)
(N.)
CHRISTMAS I. (Br.)
Cocos Is. (Br.)
Manila
LUZON
PHILIPPINE ISLANDS (U.S.A.)
MINDANAO
PALAU Is. (Jap.)
YAP (Jap. M.)
CAROLINE ISLANDS (Mand. to Jap.)
GUAM (U.S.A.)
MARIANAS Is. Mand. to Jap
OGASAWARA Is. (Jap.)
TROPIC OF CANCER
WAKE I. (U.S.A.)
MARSHALL ISLANDS (Mand. to Jap.)
MIDWAY Is. (U.S.A.)
GARDNER I. (U.S.A.)
NECKER I. (U.S.A.)
HAWAIIAN ISLANDS (U.S.A.)
Honolulu
JOHNSTON I. (U.S.A.)
GUADALUPE I. (Mexico)
C. San Lucas
Mazatlan
REVILLA GIGEDO Is. (Mexico)
Guadalajara
Mexico
CLIPPERTON I. (Fr.)
EQUATOR
PALMYRA I. (U.S.A.)
WASHINGTON I. (Br.)
FANNING I. (Br.)
CHRISTMAS I. (U.S. & Br. Claims)
HOWLAND I. (U.S.A.)
BAKER I.
JARVIS I. (U.S.A.)
MALDEN I. (Br.)
STARBUCK I. (Br.)
MARQUESAS Is. (French)
GILBERT Is. (Br.)
PHOENIX Is. (Br.)
CAROLINE ATOLL (Br.)
FLINT I. (Br.)
TOKELAU I. (N.Z.)
MANIHIKI Is. (N.Z.)
VOSTOK I. (Br.)
TUAMOTU (Low) ARCHIPELAGO (French)
NAURU (Br. Mand.)
BISMARCK ARCHIPELAGO (Aust. M.)
ELLICE Is. (Br.)
SOLOMON Is. (Br.)
SANTA CRUZ Is. (Br.)
SAMOA Is. (N.Z. Mand.)
Apia
TUTUILA I. (U.S.A.)
SOCIETY Is. (Fr.)
TAHITI
COOK Is. (N.Z.)
TUBUAI (AUSTRAL) Is. (Fr.)
RAPA I. (Fr.)
MARUTEA (Fr.)
PITCAIRN I. (Br.)
TERR. OF NEW GUINEA (Aust. M.)
NEW GUINEA
PAPUA (Aust.)
Port Moresby
CORAL SEA
NEW HEBRIDES (Br. & Fr.)
FIJI Is. (Br.)
Suva
TONGA Is.
LOYALTY Is. (Fr.)
NEW CALEDONIA (Fr.)
Noumea
Townsville
Wyndham
Burketown
Broome
Rockhampton
Brisbane
NORFOLK I. (Aust.)
KERMADEC Is. (N.Z.)
LORD HOWE I. (Aust.)
NORTH I.
AUSTRALIA
INDIAN
SOUTH
45
0
L

Checklists Aren't For Dummies, Dummy!

The Medici Effect……

“Ask the audience”

or

“phone a friend”?

mcurphey@microsoft.com