Information Security in a Flat World

John G. O’Leary, CISSP

O’Leary Management Education

Abstract

- In *The World is Flat,* Thomas Friedman tells us that connectivity and a host of innovations and activities have leveled the business playing field to such an extent that individuals in third world countries can reasonably compete with giant multinationals for contracts to provide goods and, especially, services.
- OK, but what about information security in this flat world? Is there any? Do we need some? How much? Who decides? Who manages it? How good is it? Does it work the same everywhere? Are there topological bumps in our presumably flat surface? More importantly, what can we do about all this?
- We'll answer all your questions and solve all your problems in 45 minutes. If you believe that, then the world probably is flat. For doubters, we'll try to give you an idea of and some realistic approaches for handling things you'll have to address in the near future, if not right now

Speaker Bio

- John O'Leary, CISSP, is President of O'Leary Management Education. His background spans four decades as an active practitioner in information systems, IT Security and contingency planning. John has designed, implemented and managed security and recovery for networks ranging from single site to multinational. He has been honored as a "Fellow of the Security Profession," and is a highly-rated and much requested instructor. O'Leary has trained tens of thousands of practitioners, and regularly conducts on-site programs at major corporations and government facilities worldwide. Since 1995, he has also facilitated meetings of Peer Groups, where security professionals from diverse corporations share ideas, concerns and techniques. John was the recipient of the 2004 COSAC award and the 2006 EuroSec Prix de Fidelite.
- He has never been convicted of anything really serious or run for public office.

Agenda

- The Flat World Today
- Flattening factors
  - Sourcing
  - Privacy
- Identity & Access Management
- Recommendations

The Flat World Today

- 1 billionth Internet user logged on in 2005
- Likely to have been a 24-year old woman in Shanghai
- Perhaps running a small business
- Maybe she put up her new website
- Adding to the 600 billion web pages now available
  - 100 for every person on earth

The Flat World Today

- Doesn’t matter …
  - Where you are located
  - How many employees you have
  - How old you are
  - How long you’ve been in business
  - How many products are in your catalog
  - How strong your market position is right now

The Flat World Today

- With …
  - Web Connections
  - Collaborative Computing Software
  - Service Oriented Architecture
  - Proper partners (and it doesn't matter where they are either)
  - The right product or service (niche, perhaps)
  - Adequate security (comfort level for customers)

The Flat World Today

- You can compete
  - Locally
  - Regionally
  - Internationally

  - With the locals, the big boys or anyone else

Flattening Factors (Friedman)

- Berlin Wall Coming Down
- Netscape IPO
- Work Flow Software
- Uploading
- Outsourcing

Flattening Factors (Friedman)

- Offshoring
- Supply-chaining
- Insourcing
- In-forming
- The Steroids

11/9/89

- Berlin Wall comes down
- Tipping point for free market societies
- Moved away from central planning
- Empowered individuals
- Including bad guys (Islamic militants)
- “Evil Empire” defeated by:
  - Reagan?
  - CNN?
  - Gates, Jobs, McNealy,…?
  - Bin-Laden?

8/9/95

- Netscape IPO
- 4 years after Berners-Lee invented the Web
- Universal usability, accessibility and interoperability of the Web
- Win 95 shipped 15 days later
- Number of Internet users doubling every 53 days

8/9/95

- Spawned Internet bubble
- Overabundance of fiber optic capacity
- Communication costs plummeted
- “Second buyer” (India) made out like a bandit

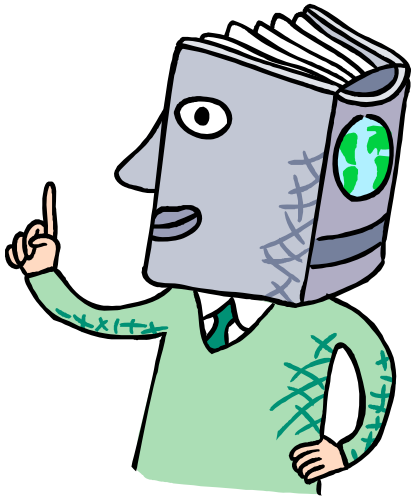
- Search for economies

Work-flow Software

- Collaboration
- Rapid development
- Rapid deployment
- Cheapest sources for coding, testing, implementation
- Everyone can create and maintain digital content
- Standards – lots of them

Uploading

- Open source
  - For production
  - Apache blessed by IBM
  - Geeks making business decisions
- Blogs
- Wikipedia



- Not controlled by corporations or Government

Outsourcing

- Y2K and India
- Talented competent programmers and engineers who will work for less
- Economic imperative
- Outsource everything you possibly can

- Seeing some backlash recently

Offshoring

- Rather than outsource jobs,
- Send the whole factory to India or China or Indonesia or …….
- Not just manufacturing
  - Management
  - Medical
  - Consulting
  - Accounting
  - ……..

Supply-chaining

- Wal-Mart is the 800-pound gorilla
- JIT to the nth degree
- Totally integrated
- IT infrastructure as a key competitive advantage
- Suppliers as partners
- RFID
- All those integrated IT systems better be up and running

Insourcing

- UPS
- Intimate collaboration
- 3rd-party managed logistics
- "They" act as part of "Your" company
  - Fixing Toshiba laptops
  - Managing delivery of Papa John's Pizza supplies
  - Packaging Segrest Farms live tropical fish for delivery
  - Picking, inspecting, packing and delivering Nike shoes
  - Same for Jockey shorts
  - Working with Plow and Hearth furniture suppliers to improve packaging and reduce breakage
- You depend on them …. totally

In-forming

- Building and deploying your personal information supply-chain
- Google – now 1 billion searches per day

- Soon “everything” will be searchable

Now

- Including everything about you and me
- And everyone’s a private eye

The Steroids

- "*Making collaboration digital, mobile, personal, virtual*" – Carly Fiorina
  - Computing capabilities - including speed, I/O rate and storage capacity
  - IM and file sharing – BitTorrent, Kazaa
  - VoIP – Skype
  - Video Conferencing – HP & SKG
  - Advanced graphics – from video games
  - Wireless – communicate with anyone from anywhere

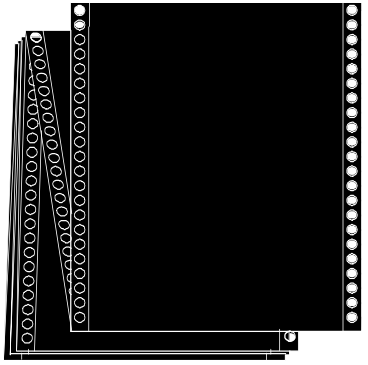
Sourcing

- Outsourcing or insourcing or offshoring
- Classic flat world strategies

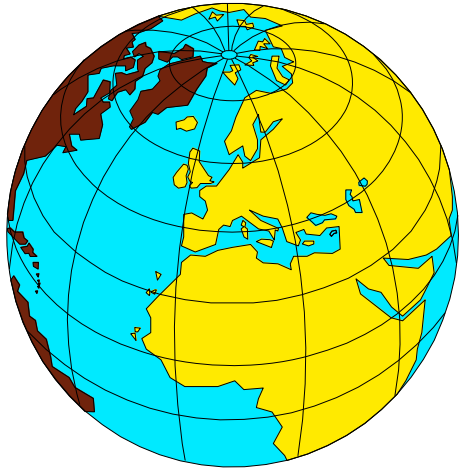
- Security issues for all of them

Security Issues

- Ownership of data
- Access approval authority
- Disclosure of sensitive information
- Security controls at vendor site



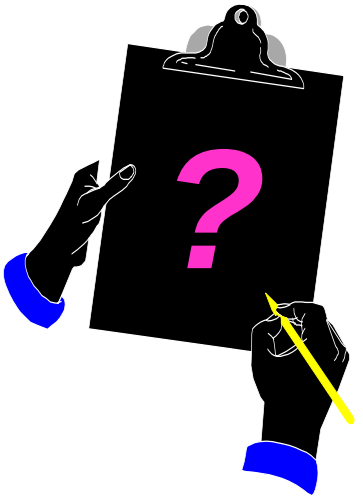
Security Issues



- Partitioning of customer data by vendor
- Network security
- Customer policies vs. vendor policies
- Laws in venues where outsourcing is performed
  - India, China, Philippines, etc.

Security Issues

- Loss of control
- Security and privacy of the customer's customers
- Staff IT & ITSec personnel
- Quality assurance
- In the 21st Century, you <u>are</u> in the Information business



Security Issues

Security administration

- Who does it?
- Vendor personnel access?
- Customer personnel access?

Security Issues

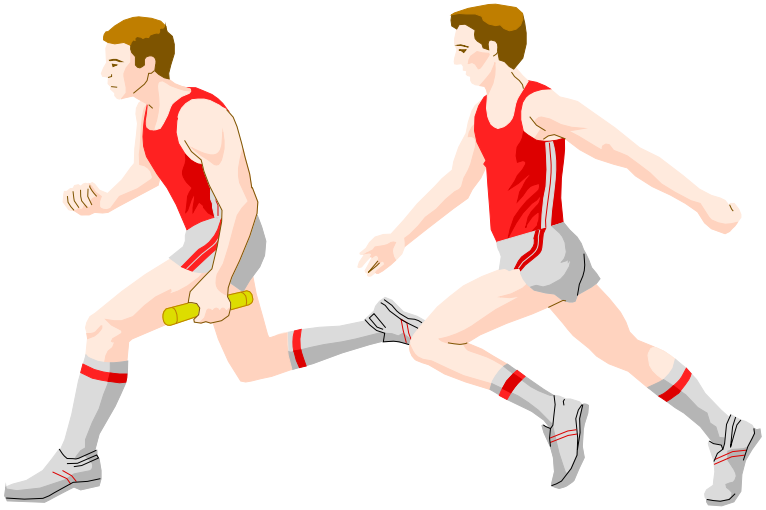
Non-outsourced items:

- Standalone PC’s
- Notebooks
- Palmtops
- LAN's
- "Special" systems
- Wireless

Security Issues

- Vendor personnel
- Lack of in-house expertise
  - analysis of proposed changes
  - problem resolution
  - incident investigation
  - future plans
- Possible union problems

Security Issues



- Level of commitment
- Audit rights and procedures
- Violation reporting and follow-up
- Security awareness

Security Issues

Viability of vendor

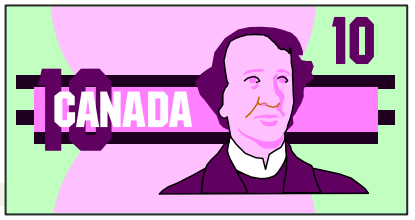
- What do you do if they go “belly-up?”
- What if they merge?
- What if they get bought?
- What if there’s a Board of Directors insurrection?
- What is your “bring it back in-house” plan

Security Issues

Viability of Vendor – Offshore

- What do you do if the government changes and the incoming one is hostile to your country or industry or company?
- What if they go to war?
- What if significant laws relating to your business being done there change?
- What if one of their citizens, in the employ of the outsourcer you contracted with, commits a crime against your customers?

Considerations



Pro

- Cost savings
- Predictable cost
- Focus on core business
- Experience and expertise of service firms
- Fewer employees (productivity)
- Insulation from internal politics (???)
- Contractual obligations and penalties

Considerations

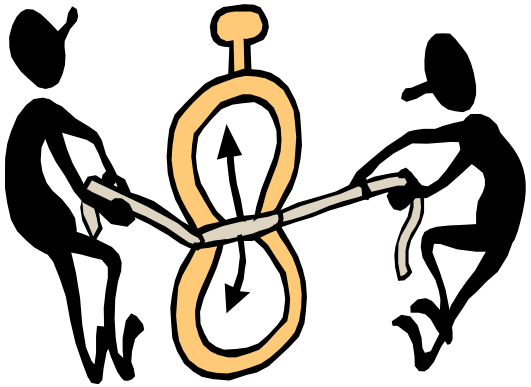
Pro

- Extend your IT staff
- Stay aware of newest and most dangerous threats
- Keep up with latest security technology, techniques and products
- Might not be inexpensive, but could be cost-effective

Considerations

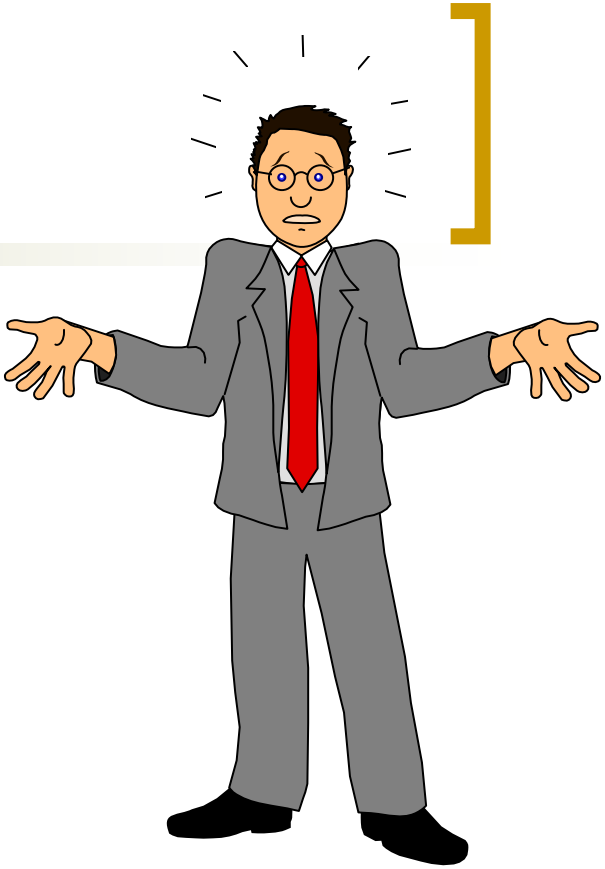
Pro

- Probably a better chance of getting help handling massive or multiple rapidly occurring problems:
- ….unless they're swamped, too
  - Storm & variants
  - New attacks
  - …



Considerations

Con



- Loss of control
- Total cost might be higher
- Loss of in-house expertise
- Increased dependence on outsourcer

Considerations

Con

- Political fallout from offshore outsourcing
  - NJ Dept of Welfare
- Privacy concerns
- Abrogation of responsibilities (?)
- Vulnerability to disgruntled or dishonest vendor personnel
  - 2005 - Indian Call Center employees (MphasiS) get CC #’s and use them

Considerations

Pro and Con

- Your firm gets as much security as it wants and is willing to pay for
- *You're* not constantly harassing people about security issues
- Perception that someone *is* worrying about this stuff …….. someone else

Privacy

- Can be very damaging and expensive if handled poorly
- Ethical issues
- In a flat world, sensitive information can be immediately available to people all over the planet
  - Authorized – with proper controls, for business reasons
  - Unauthorized – if the controls are inadequate

Privacy

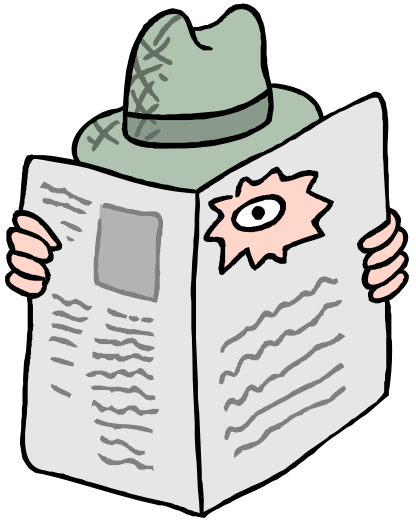
- Different laws in various parts of the world put bumps in the flat terrain
  - Japan and Canada – newest, strongest
  - Europe – led the way
  - “Meet our guidelines or we won’t do business with you”

Privacy

- Different parts of the US
  - 36 states have laws similar to Cal 1386
  - Use of SSN
  - Notification of possible breaches to all those whose PII may have been compromised
  - Federal law by end of 2008??

Privacy

- Trade secrets
- Internal plans
- Test results
- Audit findings
- Customer records
- Medical records
- Personally identifiable information
- Fraud possibilities

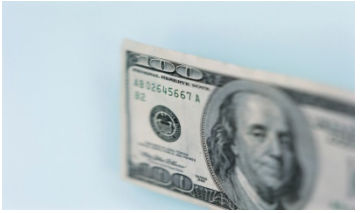


Identity & Access Management

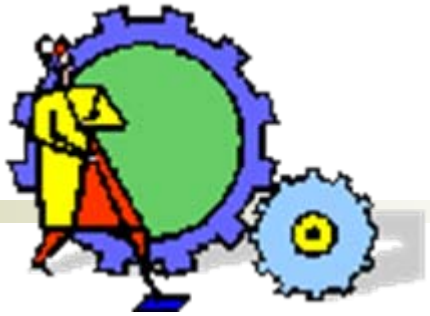
- Automation of ***processes*** ensuring that only the ***right*** people have ***correct levels of access*** to ***appropriate*** information assets of the organization
- Management and enforcement of security ***policies*** across account access domains and authentication mechanisms
- Crucial in a flat world

Identity & Access Management

- Management and synchronization of *information about individuals* across business applications
- Accurate, timely *reporting of* who made *changes* to the identity infrastructure—what, when and why
- Adherence to relevant *laws, standards, industry agreements, etc.,* relating to identity information
  - Compliance can be very expensive
  - Non-compliance even more so



I&AM



- Reusable security components
- Deployed across the enterprise
- Similar operation in all venues

- Implementation strategy is crucial
- Inter-group coordination is vital
- Audit verifies compliance
- Business “owners” responsible for granting access

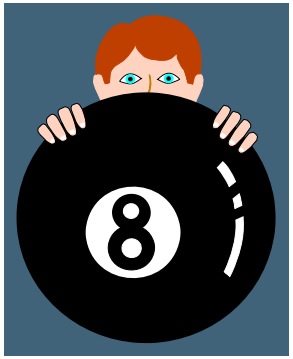
I&AM Components

- Role-based access control
- Rule-based provisioning
- Automated workflow
- Delegated administration
- Self service
- Policy enforcement through automated rule evaluation
- Robust audit and reporting

I&AM Drivers

- Cost Reduction
- Increased complexity in the enterprise (striving for simplicity)
- Heightened awareness of security

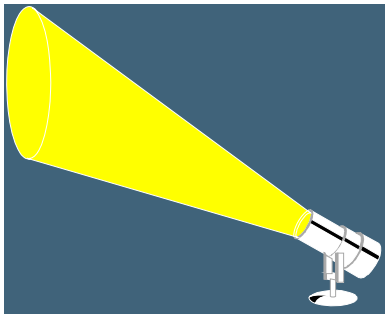
- And from the non-flat world….
- Regulation



Recommendations

- Things to do, or at least consider, when operating in a flat world
- Not a complete list
- Focus on “Sourcing” and I&AM

Recommendations - Sourcing



- Choose reputable vendors (not necessarily the least expensive)
- Conduct third party security reviews – not by your primary audit firm
- Initiate stepped-up security awareness efforts
- Perform rigorous security testing of any changes to the environment (yours and vendor's)
- Involve users in implementation plans
- Schedule frequent clarification meetings with vendors

Recommendations - Sourcing

- Draft detailed security checklist(s) for outsourcers to fill out and your security people to analyze prior to signing contracts
- Obtain solid legal representation in countries where the work is being done
  - Specialization in local contract law
- Give substantial input to recovery plans
- Participate in recovery planning exercises

Recommendations - Sourcing

- Contractual commitments on:
  - Troubleshooting response
  - Disaster recovery
  - Violation follow-up
  - …
  - …
- Penalties and remedies for non-compliance
- Clear statement of where adjudication will happen
- Inspection by customer auditors of vendor processing site

Recommendations - Sourcing

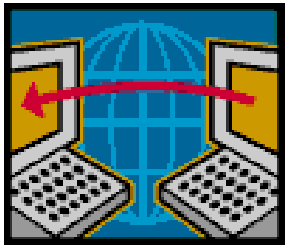
- Have a back-out plan in place
- Make sure that all security knowledge hasn’t migrated out of the organization
- Contract for independent reviews of security architecture and elements
- Perform independent customer satisfaction surveys

Recommendations (I&AM)

- Realize the strategic nature of identity and access management
- Assess its impact on your organization prior to starting the project
- Get the business people involved
- Obtain strong management support
- Focus on the people
- Start with coarse-grained authorization, then move to fine-tuned

Recommendations (I&AM)

- Remember that technology is an enabler, not the entire purpose of the project
- Define explicit security policies that drive definitions of rules and workflows
- Work toward a long term role-based and rule-based access model that allows for gradual automation of request-based processes



Summary *We have covered:*

- The Flat World Today
  - Flattening factors
    - Sourcing
    - Privacy
- Identity & Access Management
  - Recommendations

Thank you for your:

- Patience
- Attention
- Admirable restraint

- Questions
- Comments
- Rebuttals