Social Networking and Cybersecurity

NDIA San Diego Cyber Symposium
Daniel Mintz
CTO, Civil & Health Services Group
CSC

dmintz@csc.com
twitter: technogeezer

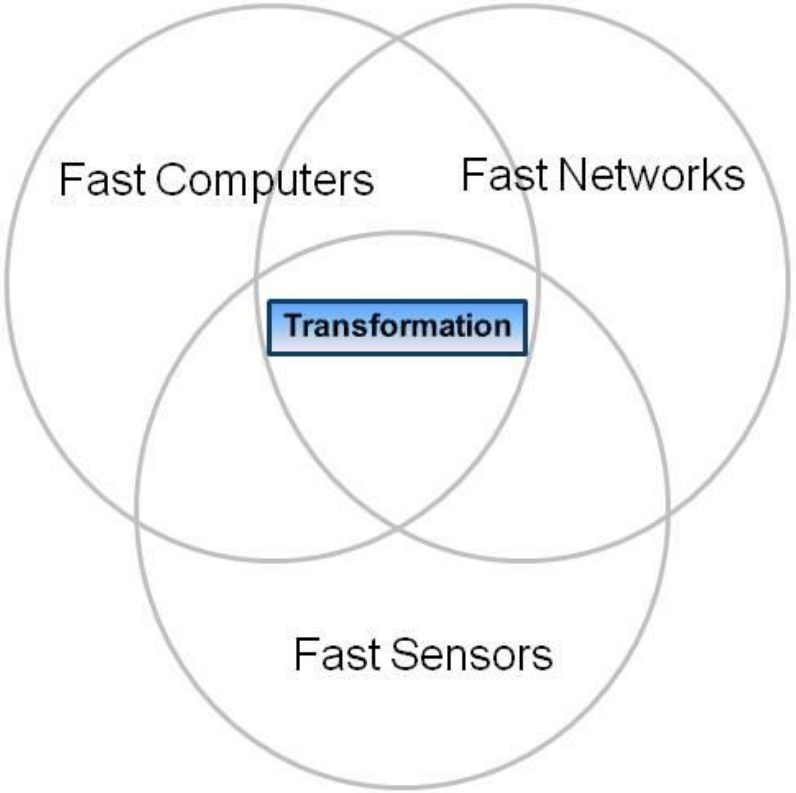
Concluding Thoughts

- You cannot maximize both data sharing and data protection completely

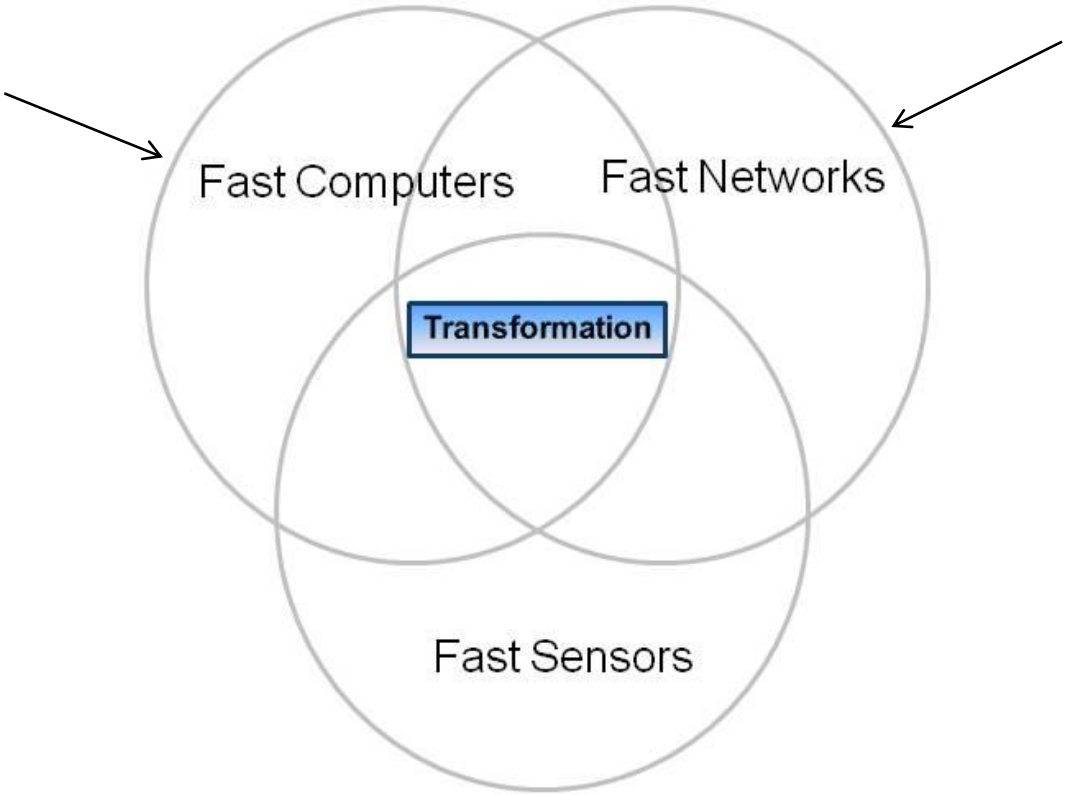
Context and Implications

- We need to keep in mind that Social Networking as we know it and Cloud Computing as we imagine it are merely a point in a continuum
- To better understand either or both it is useful to understand not just what they seem to mean now but why now
- Further we may understand a little better what will come next (though I do not)

My Version of Context



Where We Are Today



Transactional Cost Economics

- What do you know about Ronald Coase?
- He provided an explanation for the economic basis for a corporation ‘s existence
  - The higher the cost for a ‘transaction’, the more advantageous to integrate that capability internal to the corporation
- BUT – when transactional costs are reduced dramatically by the impact of the Internet, what then?
- For example, Proctor and Gamble …

The Impact of Fast Computers and Especially Fast Networks

- Social Networking
  - It is possible to create widely distributed, large networks in many geographies
  - All kinds of content can be distributed
  - The impact is bi-directional; it changes the users too
- Cloud Computing
  - It now becomes cheaper to access data centers outside than having them inside

Sample Statistics From Facebook

- More than 300 million active users
- 50% log on to Facebook in any given day
- The fastest growing demographic is those 35 years old and older
- More than 8 billion minutes are spent on Facebook each day (worldwide)
- More than 2 billion photos uploaded to the site each month
- More than 14 million videos uploaded each month
- More than 2 billion pieces of content (web links, news stories, blog posts, notes, photos, etc.) shared each week
- About 70% of Facebook users are outside the United States
- More than one million developers and entrepreneurs from more than 180 countries
- There are more than 65 million active users currently accessing Facebook through their mobile devices.

From NIST's Presentation Yesterday About Clouds

A Working Definition of Cloud Computing

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.

5 Essential Cloud Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
  - Location independence
- Rapid elasticity
- Measured service

3 Cloud Service Models

- Cloud Software as a Service (SaaS)
  - Use provider's applications over a network
- Cloud Platform as a Service (PaaS)
  - Deploy customer-created applications to a cloud
- Cloud Infrastructure as a Service (IaaS)
  - Rent processing, storage, network capacity, and other fundamental computing resources
- To be considered "cloud" they must be deployed on top of cloud infrastructure that has the key characteristics

4 Cloud Deployment Models

- Private cloud
  - enterprise owned or leased
- Community cloud
  - shared infrastructure for specific community
- Public cloud
  - Sold to the public, mega-scale infrastructure
- Hybrid cloud
  - composition of two or more clouds

General Security Advantages

- Shifting public data to an external cloud reduces the exposure of the internal sensitive data
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Redundancy / Disaster Recovery

Cloud Security Challenges Part 1

- Data dispersal and international privacy laws
  - EU Data Protection Directive and U.S. Safe Harbor program
  - Exposure of data to foreign government and data subpoenas
  - Data retention issues
- Need for isolation management
- Multi-tenancy
- Logging challenges
- Data ownership issues
- Quality of service guarantees

Cloud Security Challenges Part 2

- Dependence on secure hypervisors
- Attraction to hackers (high value target)
- Security of virtual OSs in the cloud
- Possibility for massive outages
- Encryption needs for cloud computing
  - Encrypting access to the cloud resource control interface
  - Encrypting administrative access to OS instances
  - Encrypting access to applications
  - Encrypting application data at rest
- Public cloud vs internal cloud security
- Lack of public SaaS version control

Additional Issues

- Issues with moving PII and sensitive data to the cloud
  - Privacy impact assessments
- Using SLAs to obtain cloud security
  - Suggested requirements for cloud SLAs
  - Issues with cloud forensics
- Contingency planning and disaster recovery for cloud implementations
- Handling compliance
  - FISMA
  - HIPAA
  - SOX
  - PCI
  - SAS 70 Audits

Cost of Traditional Data Centers

- 11.8 million servers in data centers
- Servers are used at only 15% of their capacity
- 800 billion dollars spent yearly on purchasing and maintaining enterprise software
- 80% of enterprise software expenditure is on installation and maintenance of software
- Data centers typically consume up to 100 times more energy per square foot than a typical office building
- Average power consumption per server quadrupled from 2001 to 2006.
- Number of servers doubled from 2001 to 2006

Cloud Economics

- Estimates vary widely on possible cost savings
- “If you move your data centre to a cloud provider, it will cost a tenth of the cost.” – Brian Gammage, Gartner Fellow
- Use of cloud applications can reduce costs from 50% to 90% - CTO of Washington D.C.
- IT resource subscription pilot saw 28% cost savings - Alchemy Plus cloud (backing from Microsoft)
- Preferred Hotel
  - Traditional: $210k server refresh and $10k/month
  - Cloud: $10k implementation and $16k/month

Back to the story

And Those Fast Sensors? They Are Happening Already

- It starts with the addition of fast sensors to the fast computers and fast networks that are now in place in much, though not all, of the country
  - Sensors become participants in the network, not just passive receptors of instructions or senders of data
  - It becomes possible to perform real-time simulations in real-time with real-time data
- And thus virtual environments and ‘real’ environments being to comingle
  - Becomes possible to emulate accurate representations of reality in real-time for interpretation and management
  - The implications are enormous and hard to predict

And Thus My Opinion of Web 3.0

- Passive Internet
- Active Internet
- Immersive Internet

And Change Is Still Accelerating

- We are more willing to admit our inability to have predicted the present than we are our inability to predict the future
- However …
  - We will guess wrong even more frequently than we do now
  - Even when right, it will often be irrelevant since we will react too slowly
  - Thus when we invest internally in such decisions we will be wasting money
- AND THEREFORE
  - We will find that the power is in the connections, not the endpoints
  - It is less important as to what, perhaps not even who, but how many you know
  - Not how much you know, but how much and how well you share
  - And all of this will have as a foundation the use of what we refer to now as social networking
- Organizations who do not adapt may fail and disappear

Who thinks that Governments will not be faced with the same dilemma and potentially with the same result?

Concluding Thoughts

- You cannot maximize both data sharing and data protection completely

From the January 16, 2009 Congressional Quarterly Today – Online News – Intelligence:

*Michael McConnell on Friday said “I believe we failed the nation at 9/11 because there was sufficient information in the system that had it been properly recognized, shared, and considered, we probably would have reacted in a different way”

“There is a constant tension between information sharing and protecting sources and methods, but as much as possible you want to share information.”

Social Networking and Cybersecurity

NDIA San Diego Cyber Symposium
Daniel Mintz
CTO, Civil & Health Services Group
CSC

dmintz@csc.com
twitter: technogeezer