Risk Management and IT

Cyber-threats, cowboys, and clouds, oh my!

Agenda

- What’s wrong with IT?
- How we can help IT
- Major risk areas, and controls
- IT governance frameworks
- Questions?

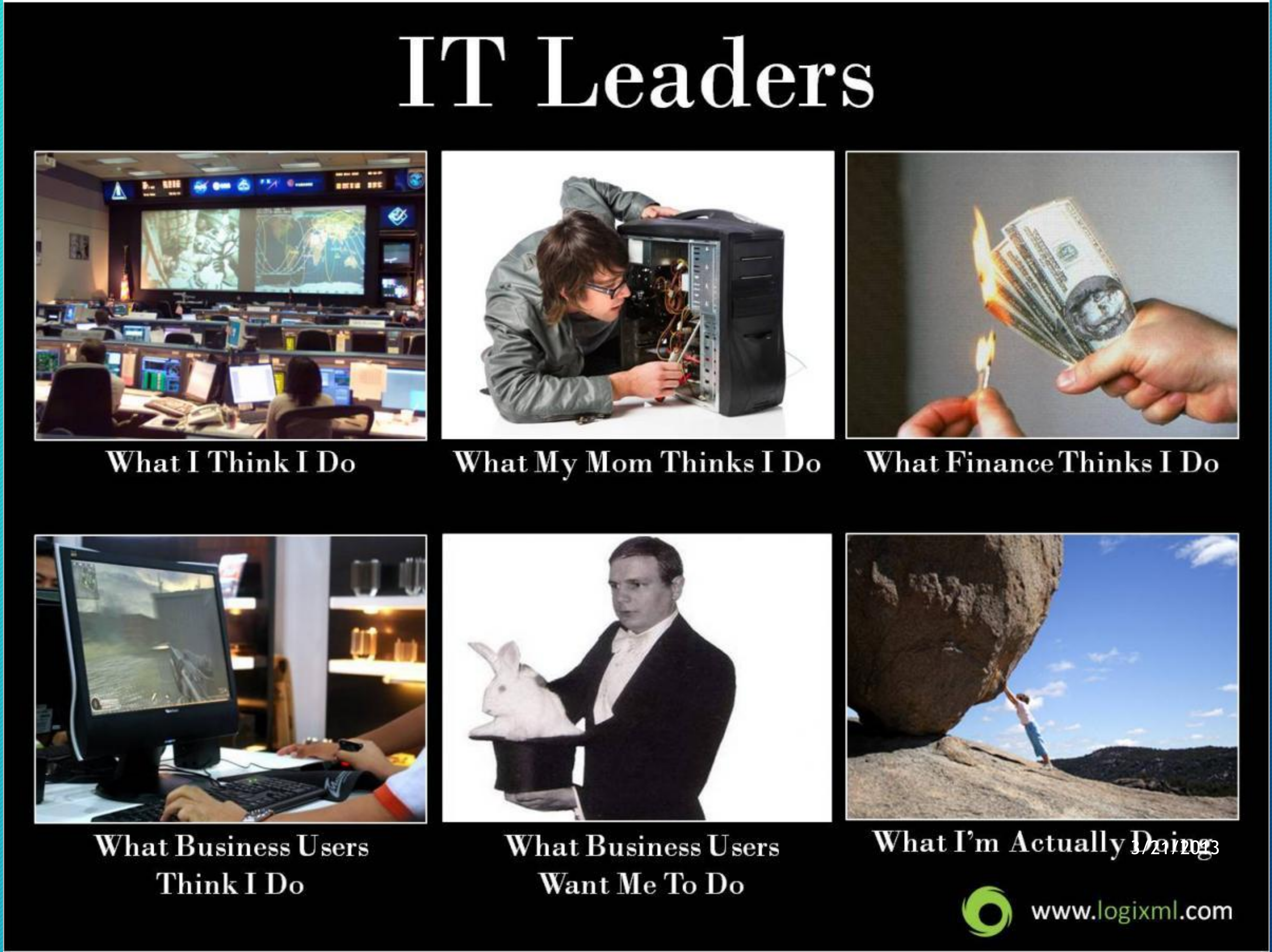
What’s wrong with IT?

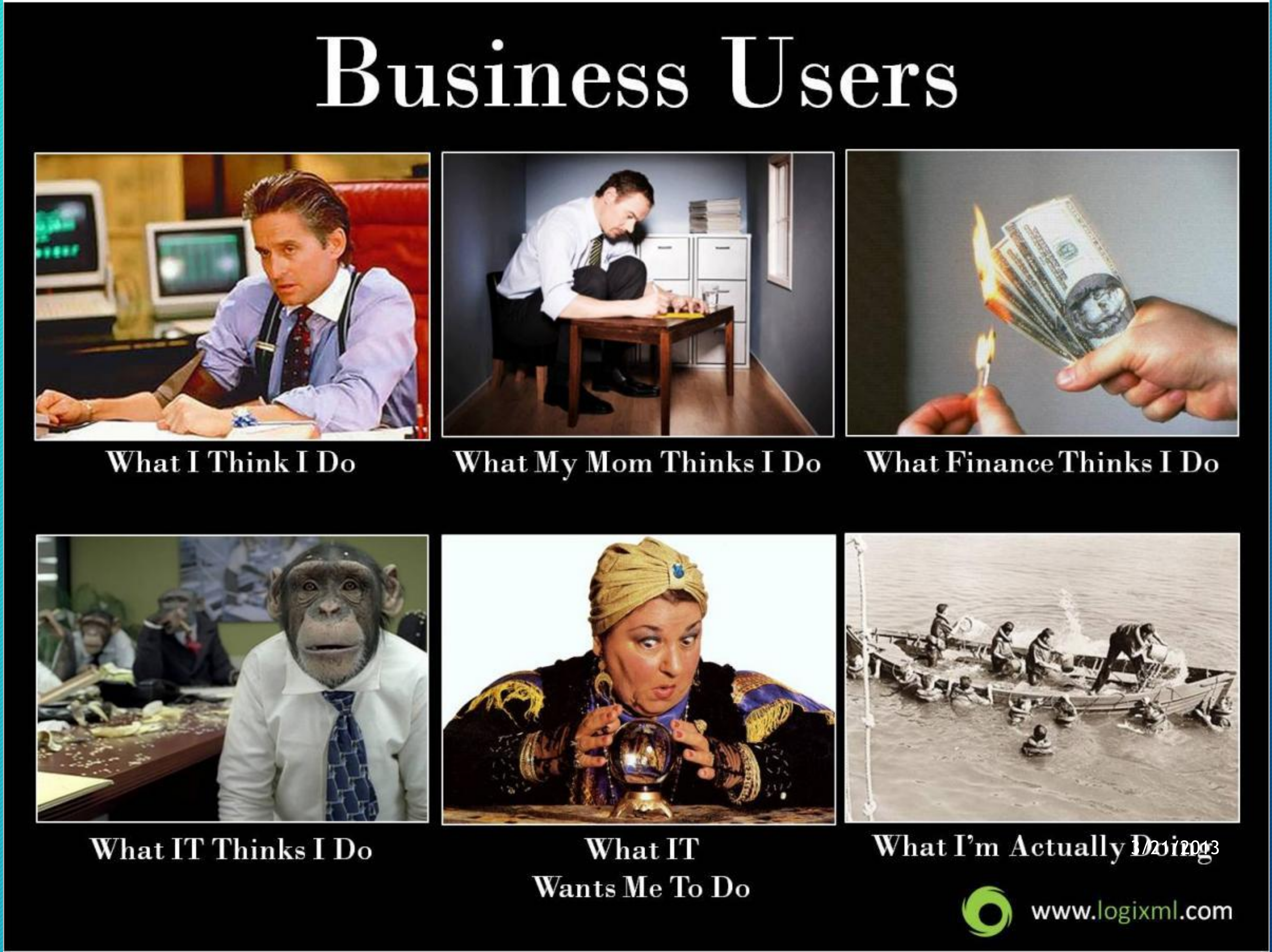
- IT is really only about 63yrs old (Internet is even less)
- Incredible rate of change
- Has a strong tribal knowledge along technology lines
  - Hardware (HP vs. Dell vs. IBM vs. …)
  - Operating Systems (Windows vs. Linux vs. UNIX, vs MacOS vs. …)
  - Applications, (etc…)
  - Mobile devices, (i.e. Android vs. Apple iOS vs. Blackberry vs. …)

What’s wrong with IT

- Management of Information Systems is even younger
  - Differing technologies make it difficult (apples and oranges)
  - Lack of common practices
  - Compared to Manufacturing or Engineering methodologies, IT is in it’s teen years

- Business tells IT, I just bought something… make it work
- Build me a house analogy…
- **IT… is an teenager with a credit card!**


IT Leaders
What I Think I Do
What My Mom Thinks I Do
What Finance Thinks I Do
What Business Users Think I Do
What Business Users Want Me To Do
What I'm Actually Doing
www.logixml.com


Business Users
What I Think I Do
What My Mom Thinks I Do
What Finance Thinks I Do
What IT Thinks I Do
What IT Wants Me To Do
What I'm Actually Doing
www.logixml.com

How we can help IT grow up

- Understanding the general problem is half the battle won.
    - You’ll also need to understand your current IT tribe
        - FIX IT! FIX IT! FIX IT!
        - Something’s not right here…
        - I don’t know where to begin…
        - We’re on the road to Service Management
        - Continuous Improvement

- Begin a Service Management strategy (i.e. start)

What is Service Management?

- "…the implementation and management of quality IT services that meets the needs of the business." *-Wikipedia*

- Focused on the **services** that all the hardware, operating systems, and applications provide as a collective whole.
- Cradle-to-grave management of the service
- Not about application or technology development
- The main tool used to mitigate risks associated with IT

“Providers of IT services can no longer afford to focus on technology and their internal organization[;] they now have to consider the **quality** of the services they provide and *focus on the **relationship** with customers.*”

IT Service Management Forum (2002). van Bon, J.. ed. *IT Service Management: An Introduction*. Van Haren Publishing. Emphasis added.

Where to start… what are the major risks

- Need to deal with the cowboys, cyber-threats, and clouds.
- These constitute the greatest risk to IT services
- IT Risk Management assesses against 3 main areas
  - Integrity = Cowboys
  - Availability = Cyber-threats
  - Confidentiality = Clouds

The Cowboy (or Cowgirl)

- Little respect or knowledge for documented quality/process.
- Very much stuck in the reactionary rut
- Always fire fighting
- Business savior (improper)
- IT tribal mentality is predominantly “FIX IT! FIX IT! FIX IT!

Main risk is to the Integrity of the service, but overlaps into Confidentiality, and Availability

The Cowboy/Cowgirl controls

- How to help them?
    - Organizational Change Management (realize it’s going to take some time)
    - You may have an entire ranch
    - Very similar process to any successful quality initiative.
    - Scheduling Proactive Time (they are stuck in a rut)
- Processes that are an absolute must to mitigate the risk
    - Incident & Problem Management with KPIs
    - Change Management (representation from key users/stakeholders)
    - Eventually system/service design and test

The Cyber-Attacker

- Perceived as externally facing, but majority of incidents are internal
  - User let’s kids play on work computer, get’s a virus, attaches to the network.
  - Disgruntled/terminated staff
  - Network Surfing
- Data Loss & Recovery (i.e. Backups)
- Keeps the Cowboys/Cowgirls fighting the fires
- Social Engineering
- Increasing everyday and becoming more sophisticated

Main risk is to Availability of the service, but is very close to both Integrity and Confidentiality.

The Cyber-Attacker controls

- How do we NOT help them?

- Security Awareness program (esp. around Social Engineering)
- Make sure to be using the basics; Anti-Virus, Firewalls, Patch Management (together with Change Management)
- Acceptable Use Policy
- CSIS-20 “20 Critical Security Controls for Effective Cyber Defense” (www.sans.org)
- Create a Security Management system (ISO27001)
- Disaster Recovery & Business Continuity processes (ISO 22301)

The “Cloud”

- Nothing really new about the cloud
  - E-commerce
  - Web 2.0
  - Utility/Grid Computing
  - Virtualization / Server Consolidation
  - ASP
- Marketers finally found a name that people liked.
- Does have compelling service drivers, cost, ease of access, etc..
- Main risk is Confidentiality, followed closely by Availability

The “Cloud” controls

- Very important to understand the impact of the information you are storing in the cloud
- Bring Your Own Devices (absolute need of an AUP around BYOD)
  - Some companies opt for secure “container” on the device
- Understand who you are giving your data to, and what controls they have in place.
  - Are they open to an audit to verify/validate compliance?
- Use can mitigate risks in some areas but create additional risk in others (i.e. Internet connection dependence)
- Make sure to have detailed Service Level Agreements(SLA) in place

Common Governance Frameworks

- Information Technology Infrastructure Library (ITIL)
  - Currently in revision 3
  - Most common and adopted framework
  - Brings common terms and definitions
  - Created by the UK Government Office of Commerce (OGC)
  - Details the how and some general flow
  - Poor alignment with other standards (COBIT, ISO2700x, ISO900x, CMMI)
  - Caveat is making your business fit ITIL, instead of the other way around.

Common Governance Frameworks

- Control Objectives for Information and Related Technology (COBIT)
  - Very business goals orientated. Strong linking between business goals and IT goals
  - Has checklists and what we would expect results to be.
  - Contains other processes (i.e. Project Management)
  - Aligns well with other standard and practices (ITIL, ISO27000, CMMI, PMBOK)
  - Most common used framework to comply with Sarbanes-Oxley Act
  - Created by ISACA. Currently in revision 5

Other Governance Frameworks

- ISO20000 – IT Service Management
- ISO38500 – Corporate Governance of Information Technology
- GAMP – Good Automated Manufacturing Practice (used primarily in the Pharmaceutical Industry
- Microsoft Operations Framework
- (Insert your favorite framework here)

- Important thing to remember is that these are frameworks, not prescriptive guidance.

Risk Management and IT Conclusion

- Start with a business case and establish clear objectives/requirements
- Include a Risk Assessment (NIST 800-30 is a good resource)
- Join up with some of the LinkedIn groups on IT governance
- Ask for help

Questions?

UO SYSTEM
Management

Ben Habing

Tel: 780-756-1401

E: bhabing@uosystem.com

W: www.uosystem.com