RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Security of Large Technical Systems

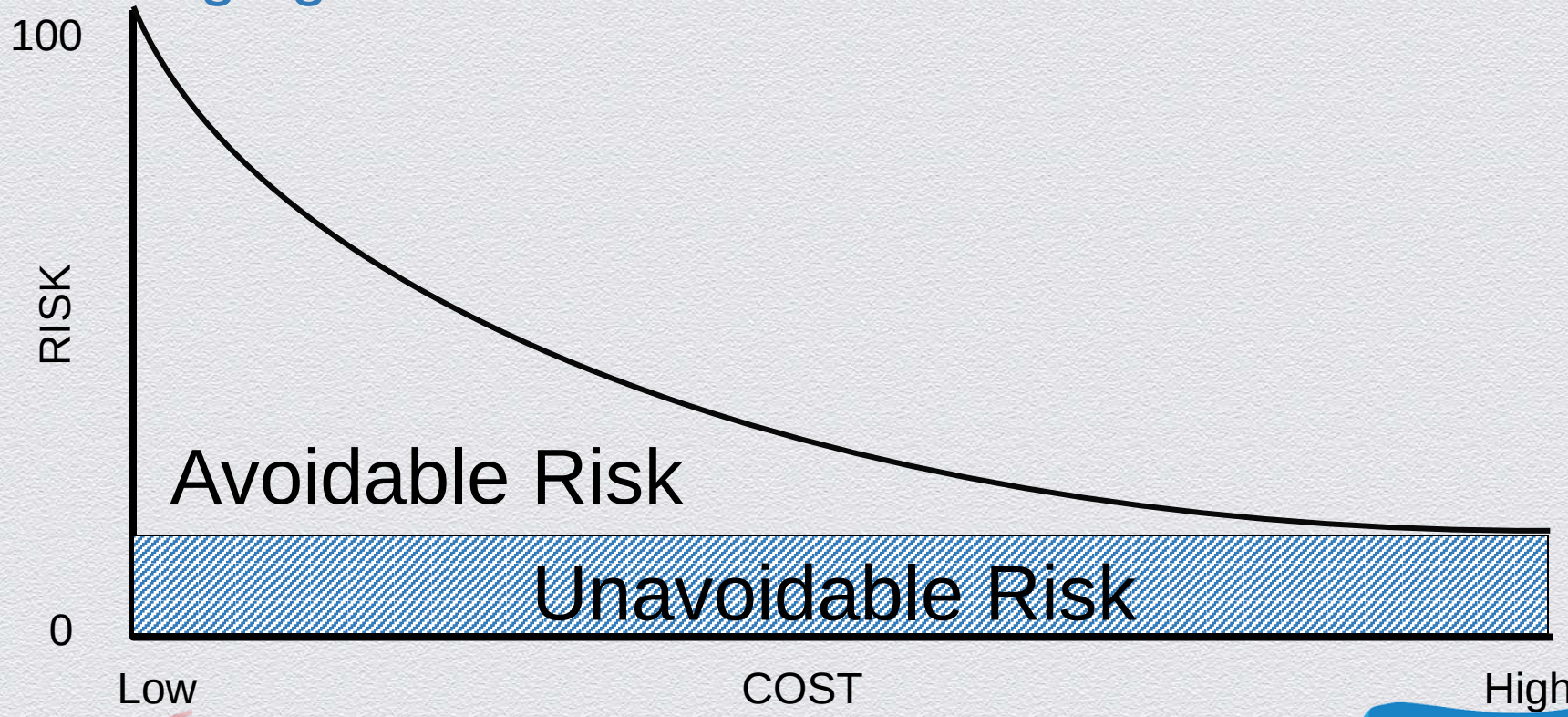
SESSION ID: STR-W02

Marcus H. Sachs, P.E.

Vice President, National Security Policy
Verizon Communications
@marcussachs

Before We Get Started….

Managing Risk

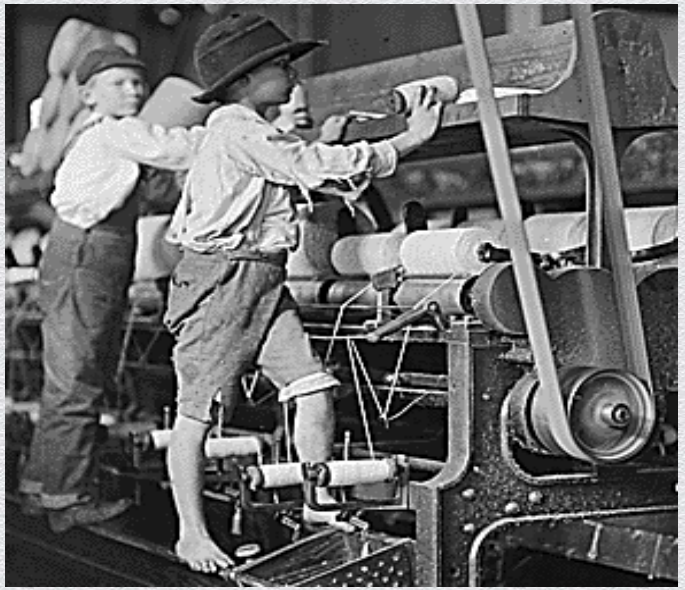


Introduction – The Industrial Age

- Development and growth of machinery and technology designed to simplify or replace manual tasks
- Early simple methods of mechanization and automation led to today's highly complex systems
- Required new techniques for control and management to prevent catastrophic failure or destruction
- Governments and legal systems reacted in various ways, not always positive

Industrial Age Technologies

- Late 1700s Textiles, iron making, and steam power
- 1793 Cotton gin
- 1807 Steamboat service
- 1812 Gas lighting in cities
- 1825 Steam locomotive and railways
- 1836 Telegraph
- 1858 Internal combustion engine
- 1866 Transatlantic cable
- 1876 Telephone
- 1879 Light bulb
- 1888 Electric motor
- 1892 Diesel engine
- 1903 Airplane
- 1913 Automotive assembly line



The Growth of Large Technical Systems

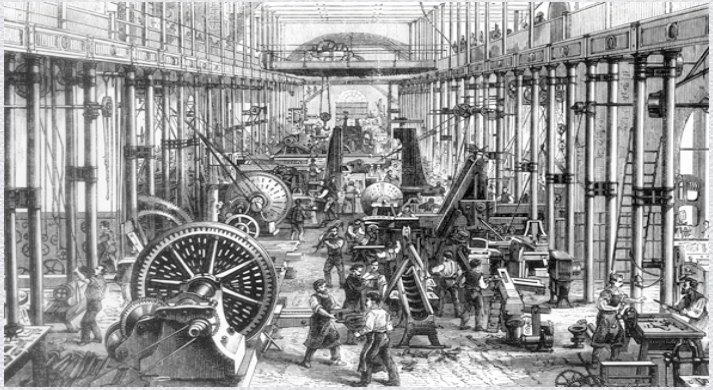
- The post-World War II era, especially the early years of the Cold War, were characterized by an explosion of Large Technical Systems (LTSs)
  - Term was coined by technical historian Thomas Hughes in his 1983 book "Networks of Power: Electrification in Western Society 1880 – 1930”
- LTSs brought together pieces invented during the Industrial Age
  - “Intelligent control” was needed to manage an LTS
  - Computers, both analog and digital, became the “brains” of an LTS

Examples of Today's Large Technical Systems

- Railroads, highways, shipping canals
- Air travel (traffic control, reservations, fly-by-wire aircraft)
- Communications networks
- Energy grids (electric, gas, petroleum)
- Banking and financial systems, including computerized stock trading
- Space vehicles and support systems
- Nuclear missile early warning systems
- Nuclear power (fuel as well as the facility)
- Just-in-time package delivery

Industrial Age LTSs

- Early LTSs were easy for an average person to understand
  - Mostly mechanical in their construction, with linkages, wheels, cams, rods, levers, switches, relays, and other devices
  - *Simulated various physical parts of the human body* (arms, legs, elbows, fingers, etc.) only on a much grander scale



- Mechanical LTSs were linear, rational, and predictable
  - Internal feedback and control mechanisms were also mechanical

Information Age LTSs

- Modern LTSs are “complex” and follow different behavioral rules from earlier LTSs
- They are no longer just large semi-predictable mechanical systems
  - They are non-linear, non-mechanical, non-rational systems that are typically controlled by one or many computerized “brains”
- They are systems that are increasingly based on artificial intelligence rather than just artificial muscles and bones

How Do You Govern and Control Complexity?

- Today's LTSs might do unpredictable things
  - This is characteristic of chaotic systems
- In fact, we have likely moved to an era of Large Technical *Chaotic* Systems
- If true, it might help explain some of the difficulties organizations face with respect to understanding and mitigating external and internal threats that target today's LTSs
  - Organizations are like assembly line processes
  - Linear, rational, predictable
  - Very much like a 19th Century mechanical system

Characteristics of Complex Systems

- A relatively new area of mathematical and scientific research focuses on chaos theory and complex systems
- Some characteristics have been identified:
  - Emergence – similar in form and structure at both fine and large scales
  - Non-linearity – the sum behavior of the parts is not necessarily the same as the predicted behavior of the whole
  - Adaptive – changes behavior in response to its environment
  - Interdependence – relationships between the behavior of sub-parts

Complexity leads to

- System collapse into smaller simpler collections.
  - Micro-grids and islanding (think about nuclear power plants)
  - Walled gardens

OR

- Unpredictable behaviors emerge
  - New integration (“just in time” delivery)
  - System failure (cascading service outages)
  - Government failure or regime change (Ukraine, Egypt, etc.)

First Problem:
Linear vs Non-linear Management

- Governments and most business organizations are mechanical and rational
- Most are based on organizational theory developed during the Great Depression
  - Optimized in the era of mechanical LTSs
  - Lessons learned from the Ford Motor Corporation's operation and management of their automotive assembly lines greatly influenced the thinking of government and business leaders in the 1930s
  - Today's bureaucratic hierarchy still reflects that thinking
- But today's society and certainly today's LTSs do not mirror the 1930s
  - Neither do the threats against our critical infrastructures, which have become just as complex in their organization as the attack and exploitation tools available to them

Second Problem: Humans Cannot Manage Complex Systems

- Large industrial-age mechanical systems were easy for people to understand and control
  - Steam locomotive (or an entire railroad)
  - Ford Model T (or a Ford assembly plant)
- Today we have highly complex and interdependent infrastructures, platforms, and systems
  - Energy grids
  - Financial systems
  - Fly-by-wire aircraft (and even automobiles)
- Computers and computer systems are needed to manage what is beyond the capacity of a person
- But what happens when the computer systems fail?

Air France Flight 447, May 2009

- Airbus A330-200 lost communication about 3-1/2 hours after take-off from Brazil
  - Pilots lost control of the aircraft as it passed through thunderstorms over the Atlantic
  - Black boxes and other computer systems were found two years after the event
- A330 is a “fly by wire” airframe that uses three primary and two secondary computers
- Pilots argued with each other about what was wrong, all the way to impact

Washington, D.C. Metrorail Crash, June 2009

- Metrorail crash avoidance system failed to stop a south-bound train
- Investigations revealed that the system had failed more than once prior to the crash
  - Of 668 incidents that caused delays in 2008, track circuits accounted for 337
- At the time of the crash, the train speeds were set by an on-board computer
  - The train operator attempted to stop the train with the emergency brakes, but did not override the computer

Sayano-Shushenskaya Dam, August 2009

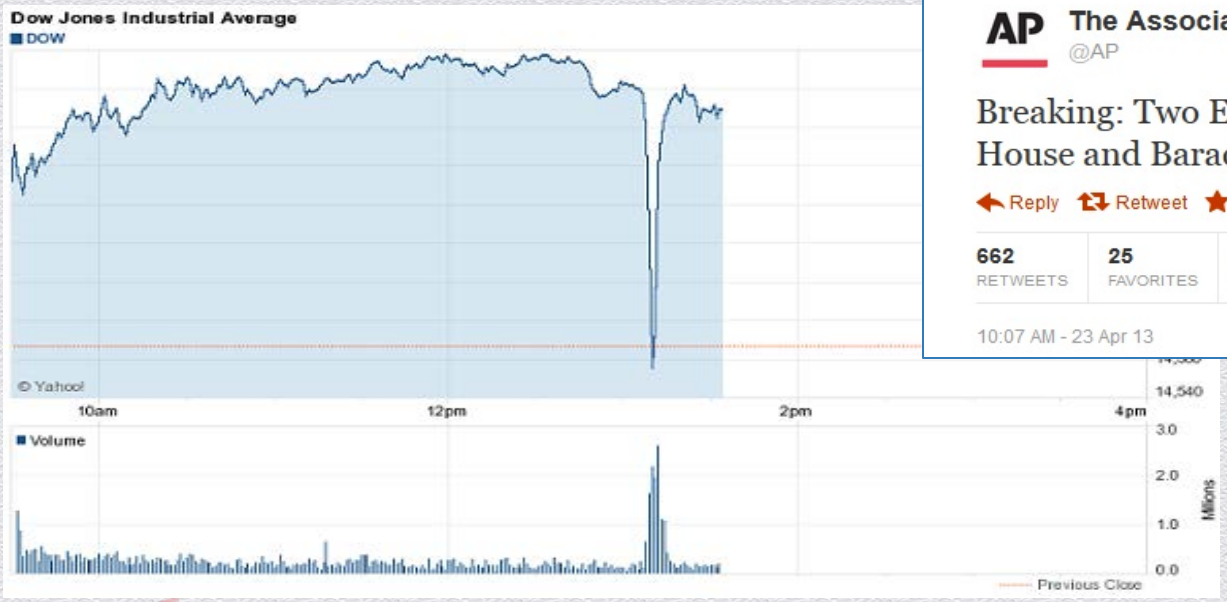
- Before the accident, was the largest hydroelectric plant in Russia, sixth largest in the world
- The 920-ton rotor of turbine #2, known for several years to have mechanical problems, lifted out of its seat
- Computers failed to shut down the turbine
- Water flow had to be manually turned off

NYSE “Flash Crash,” May 2010

- Fortunately no loss of life
- DOW dropped more than 600 points in five minutes, then regained the 600 points in 20 minutes
- Triggered by a large mutual fund firm selling an unusually large number of E-Mini S&P 500 contracts
- “Crash” resulted from actions taken by computerized trading system

Social Media Impacts Stock Market, April 2013

- AP Twitter hack results in a 1% drop of the DOW

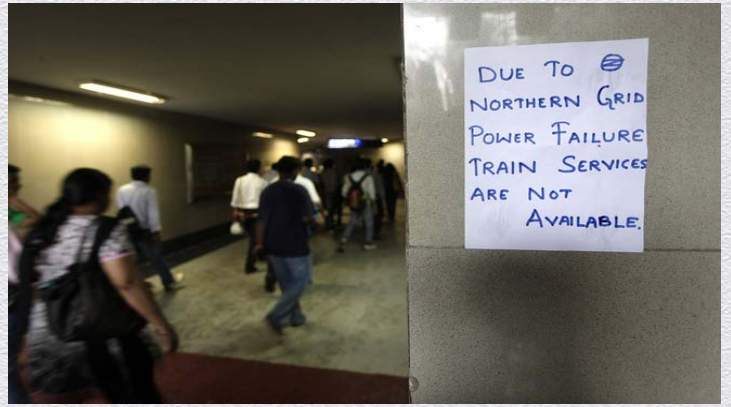


NASDAQ, August 2013

- “Flatlined” for about three hours due to software problems

Collapse of Northern India's Power Grid, 2012

- Two back-to-back days of grid collapse
  - 680 million people without power
  - Business losses estimated in the hundreds of millions
- Cause of failure attributed to overloads, lack of maintenance, improper balancing
- Impacted electric trains, underground mines, hospitals, and government services
- Indian power minister was promoted



Asiana Flight 214, July 2013

- Boeing 777 crashed while landing at San Francisco
- Aircraft was approaching too slow and too low
- 777's can be computer-controlled from gate to gate, however the ILS on runway 28L was out of service

Other Examples

- 1986 and 2002 Space Shuttle mishaps
- 1986 Chernobyl nuclear reactor meltdown
- 2003 Canada/US electric power blackout
- 2008 Spanair flight 5022 crash on takeoff
- 2010 explosion and sinking of the Deep Water Horizon oil rig in the Gulf of Mexico
- 2011 Fukushima Daiichi nuclear power plant in Japan
- 2013 Fertilizer facility explosion in Texas

Third Problem:
Security Itself is Complex

- For cyberspace, security is not just a technical problem
  - BGP, DNS, SMTP, FTP, SSH, etc.
  - Buffer overflows, SQL injection, use of an extra “goto” statement...
- It’s really about solving a multi-dimensional risk management equation with variables that sound like:
  - Policies
  - Users
  - Software
  - Hardware
  - Networks

$$R(x) = Px^a + Ux^b + Sx^c + Hx^d + Nx^e$$

$$X_{n+1} = Px_n(1-x_n) + Ux_n(1-x_n) + \ldots$$

Is Failure an Option?

- A better question might be, “is failure normal?”
- If we agree that Large Technical Complex Systems can, and will, fail for any number of reasons – then how do we manage that risk?
  - Should we strive to prevent failure?
  - Or should we try to manage failure?
- Remember the risk curve we talked about earlier
  - Perfect security (or safety) is rarely achievable
  - Best to understand your risk tolerance level, then manage risk to that level

Some Possible Solutions

- Start with organizational theory
  - Are we set up for failure because of the way we govern? If so, this is a policy problem!
- Next look at how we respond
  - A top-down bureaucracy model is linear and slow to adapt
  - Ad-hoc security coordination is more like a chaotic system, but will it work under stress?
- Then consider modifying the technologies
  - Fundamental flaws with software and hardware
  - Basic network mechanism weaknesses are everywhere

Bringing Good Minds Together

- "More information sharing" is a current policy theme
- Today, most is linear or one-way sharing
  - Old saying: "Tell me everything you know and we'll keep it all a secret."
  - What we should be saying: "Here is what we know. What do you know?"
- Need to synthesize knowledge by mixing what appears to be unrelated information
- Consider starting with confidence building
  - Go beyond "trust but verify"

Why is Information Sharing so Hard?

- No common taxonomy
- Differences in technology
  - And differences in the understanding of technology
- Legal barriers
  - Liability
  - Anti-trust
  - Privacy (ECPA in particular)
- But even if those legal barriers are removed, cultural issues will remain
  - Information is power; sharing is seen as a loss of power
  - Trust is hard to build but easy to destroy

Encouraging Participation

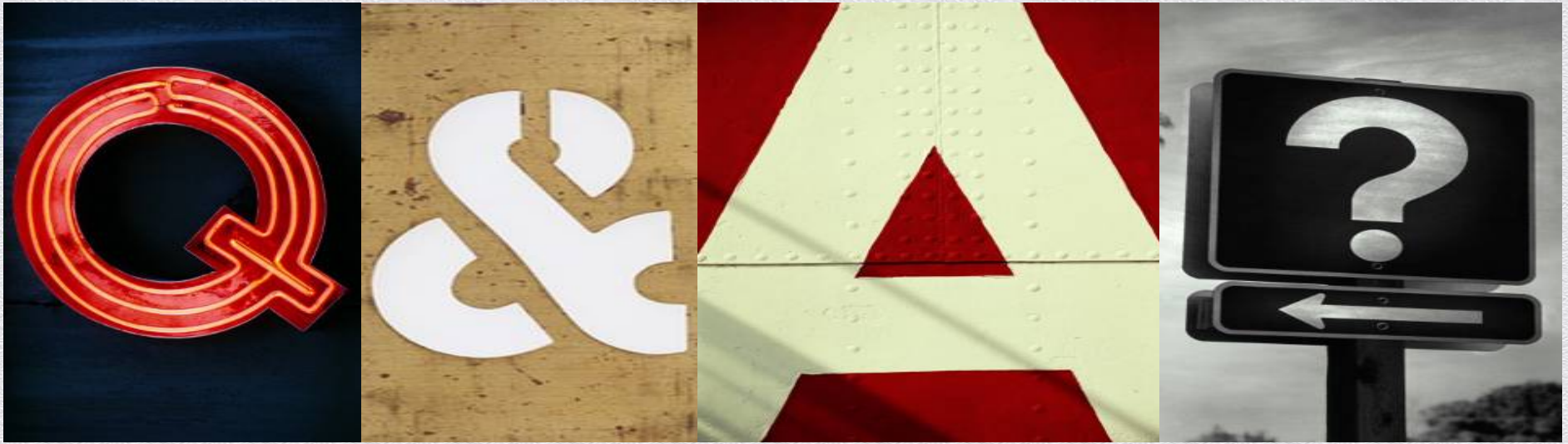
- To get participation, we must create a “value proposition” in terms that the data-holders can work with
  - If information is needed from a business, then provide some sort of ROI analysis
  - If information is needed from a government organization, then show how sharing will enhance or support that group’s mission
- Mandatory reporting IS NOT a workable approach
  - Look for incentives that support collaboration and sharing; lessen the risk of participation; show the ROI

Information sharing is also a complex problem that needs a new approach for cooperation between organizations

Summary

- Industrial Age large technical systems were mostly linear, predicable, and rational
- Information Age large technical systems tend to be non-linear, unpredictable, and irrational
- Failure WILL happen, and often in ways that were not foreseen
- The challenge seems to be based on old ways of managing systems
  - Linear organizations
  - Predictable responses
  - Rational and deliberate analysis
  - One-way information sharing

Be Mindful of Emergent Behaviors


Q
&
A
?