Inherent Unaccountabilities in Computer System Development and Operations

Mike Jerbic, CISSP, PMP

April 20, 2004

CFP 2004

CFP 2004, April 20-23, 2004, Berkeley, CA

Why talk about Accountability?

- Liability is the structured enforcement of accountability
- Accountability in the Information Age is necessary and if we’re to have freedom and privacy
- Information Technology management, engineering, and operations practices are full of unaccountable activities

Liberty means responsibility. That is why most men dread it.

–George Bernard Shaw

When Institutional Accountability Fails

My purse was stolen in December 1990. In February 1991, I started getting notices of bounced checks. About a year later, I received information that someone using my identity had defaulted on a number of lease agreements and bought a car. In 1997, I learned that someone had been working under my Social Security number for a number of years. A man had been arrested and used my SSN on his arrest sheet. There's a hit in the FBI computers for my SSN with a different name and gender. I can't get credit because of this situation. I was denied a mortgage loan, employment, credit cards, and medical care for my children. I've even had auto insurance denied, medical insurance and tuition assistance denied.

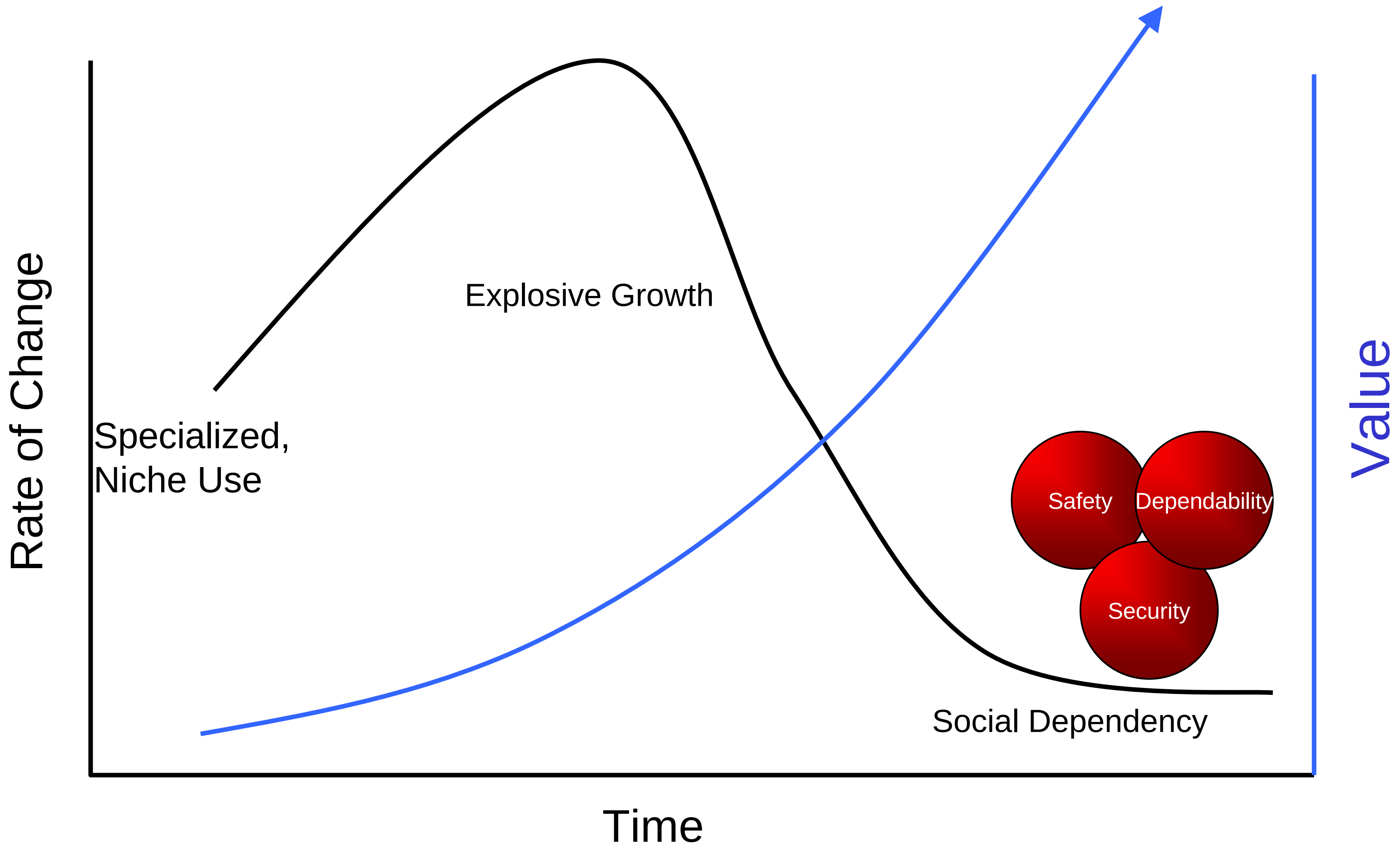
From a consumer complaint to the FTC, January 2, 2001

Identity theft is a serious crime. People whose identities have been stolen can spend **months or years — and thousands of dollars** — cleaning up the mess the thieves have made of their good name and credit record. In the meantime, **victims may lose job opportunities, be refused loans for education, housing, cars, or even be arrested for crimes they didn't commit**. **Humiliation, anger and frustration are common feelings victims experience as they navigate the arduous process of reclaiming their identity**

http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#intro

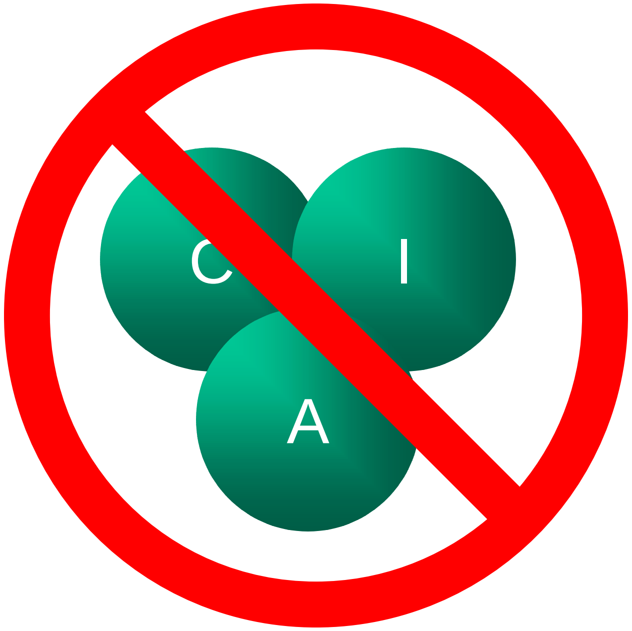
Failure of institutional accountability is tantamount to oppression

Technology Adoption



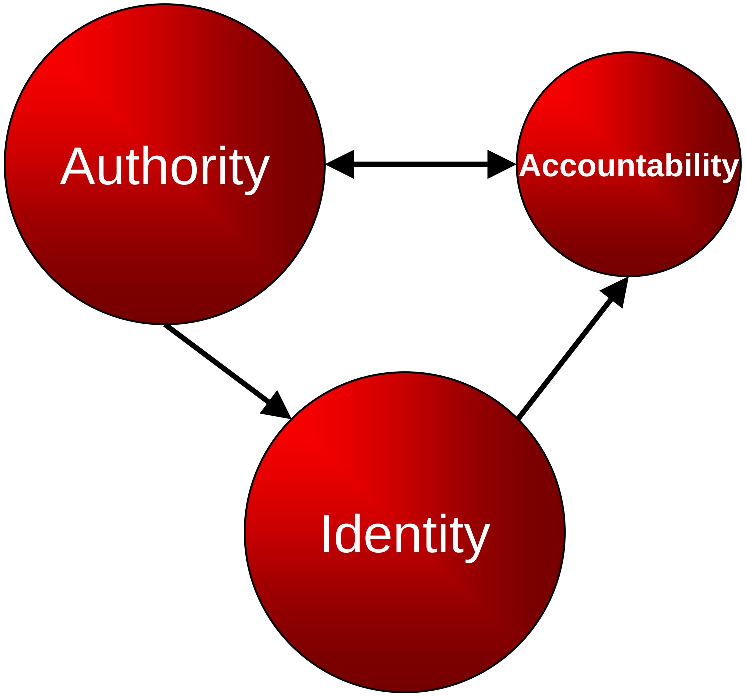
What is Security?

Classical Security Technology

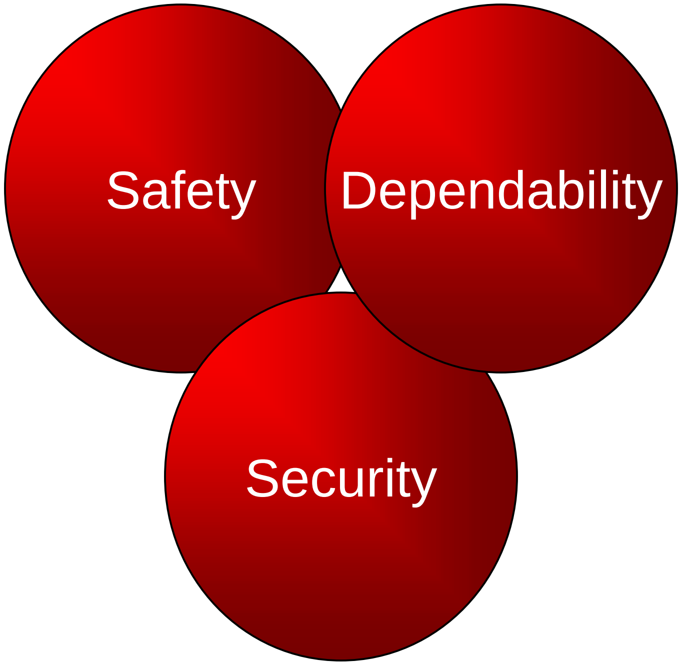


Confidentiality
Integrity
Availability

Social Problem



Accountability for Mission-Criticality is Not Just About Security



- Liability is not just about unsecured systems. It's about managing risk to an acceptable level.
- Different communities have different ideas on what an acceptable risk level is!

Accountable Parties

- Business Leadership
  - Motivation
  - Free Markets
- Product Engineering
  - Processes
  - Economic Forces
- Product Operations
  - Processes
  - Economic forces
- Government
  - Reactivity
  - Function

Business Leadership

“The highest use of capital is not to make more money, but to make money do more for the betterment of life.”

- Henry Ford

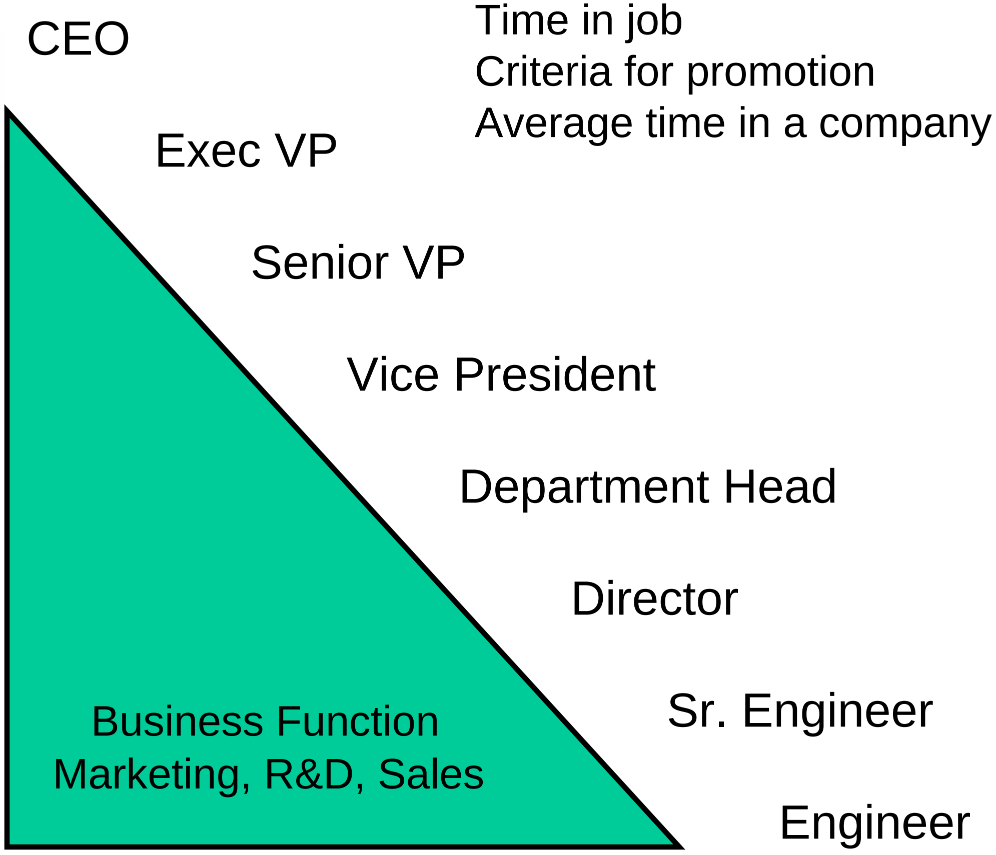
“Greed is good.”

- Gordon Gekko, Wall Street

- Motivation
  - Personal
  - Enterprise

Personal Motivations

Time in job
Criteria for promotion
Average time in a company or business



CEO

Exec VP

Senior VP

Vice President

Department Head

Director

Sr. Engineer

Engineer

Business Function
Marketing, R&D, Sales

How to (Personally) Grow in Business…

- Plan for Frequent promotions
  - Change jobs every 2-3 years
- Make short term, visible contributions
  - Make it look good now, whatever the cost later
- Manage upwards
  - Optimize work for short term visibility upwards in the organization.
- “It’s better to look good than to feel good.”

  - “Fernando” of Saturday Night Live

Enterprise Success Factors

- Enterprises often run by MBAs, not subject matter experts
- Early market entry captures customers
  - “No one ever went broke underestimating the taste of the American public.” Henry Louis Menken
- Quarterly cost driven decision making
  - Cost of regulatory compliance compared to non-compliance
  - No time to do it right, but time to do it over
    - Patch, Patch, Patch
- “Externalization” of certain costs
- Enterprises not accountable for the public’s assumption of very large risk. The more successful the enterprise, the larger the public risk

Engineering

If the automobile had followed the same development as the computer, a Rolls-Royce would today cost $100, get a million miles per gallon, and explode once a year killing everyone inside.

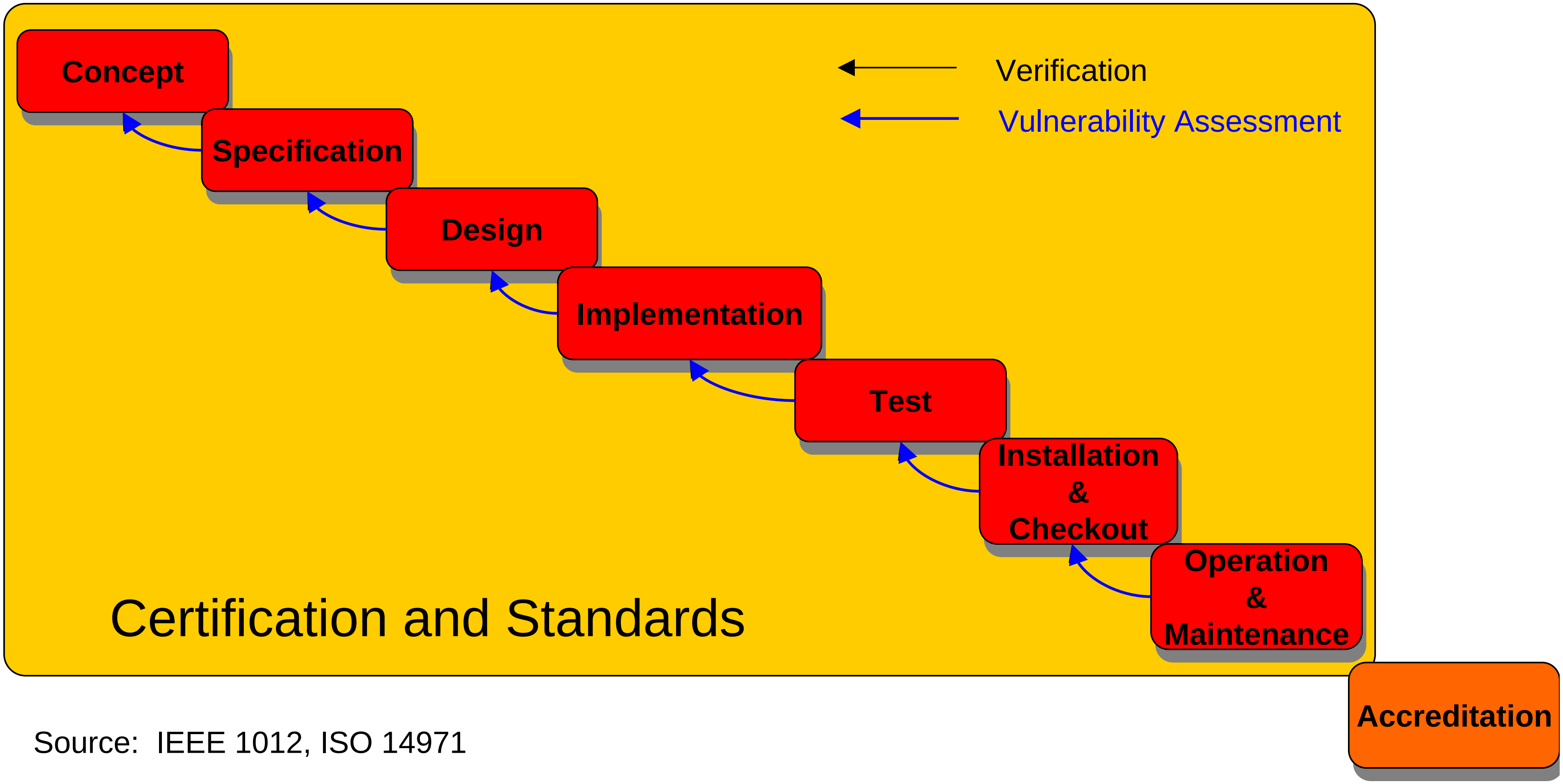
Robert Cringely , InfoWorld

- Education
- Cultural badges of honor
  - Work hours
  - Diet ☺
  - Hero worship
- Productivity/success measurements
  - Features first
  - Innovation and opportunity
  - Fix it later
- Prestige of coders versus testers
- Product release criteria
- “The Hands On Manager”

St George's implantable axilla cardiac pacemaker, English, 1967.

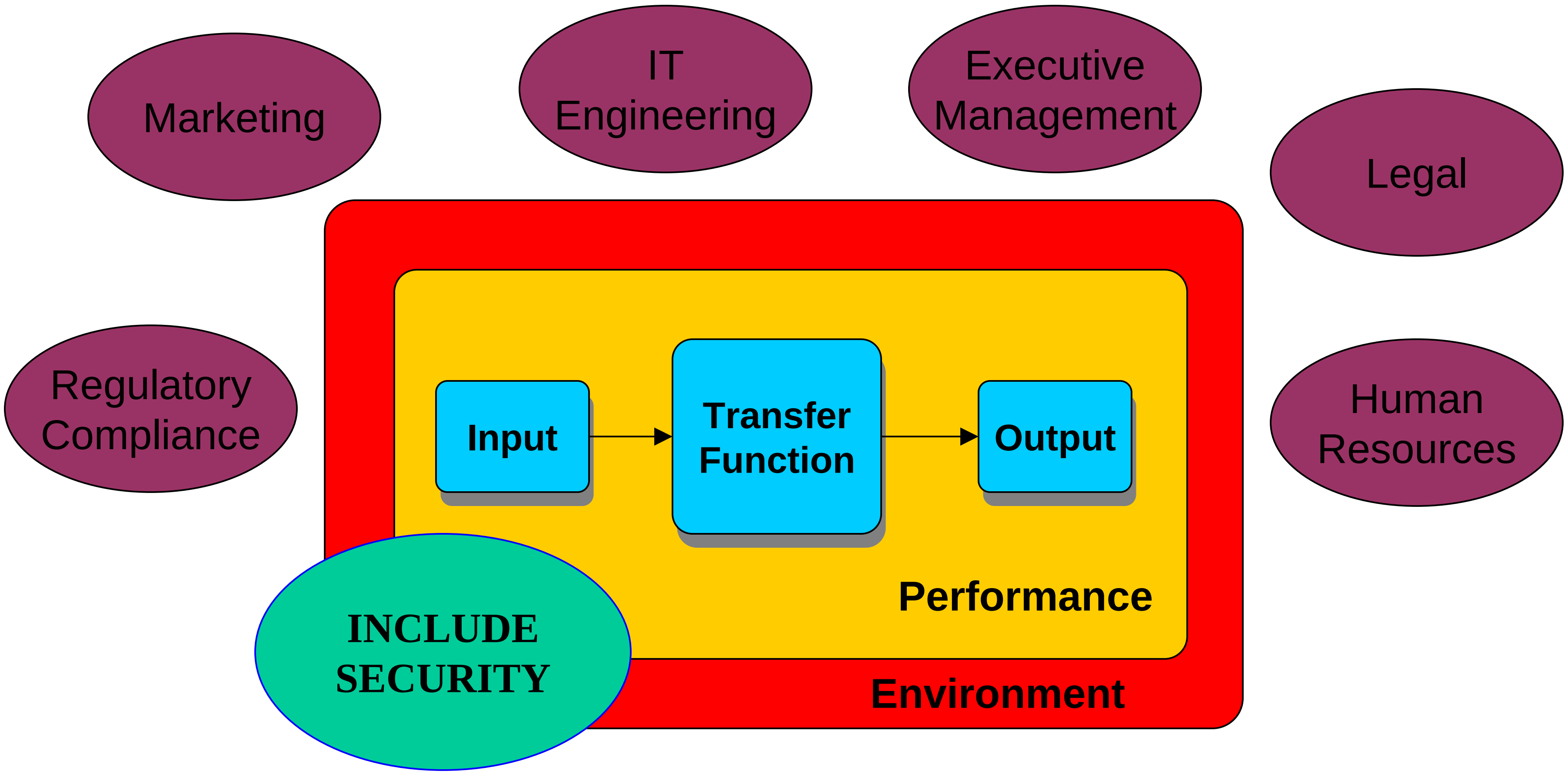
What if we built pacemakers this way?

But, We Know How to Build Pacemakers



Source: IEEE 1012, ISO 14971

Secure System Characterization



Operations

- Unanticipated risks of using technology in new ways
- System Longevity and Legacy
  - Unlike other products, old information technology never dies; it just gets upgraded
- Externalization of risks
- Best summed in a case study

Remember Identity Theft?

- Business transactions using existing card technology across the internet – increased risk
  - Too slow and expensive to upgrade credit infrastructure
- Financial institutions externalize the risk:
  - Interest rates go up to recapture fraud
- Financial institutions make false credit reports based upon unauthenticated information
- Victims inappropriately held accountable spend months of their lives and thousands of their dollars setting the record straight

Anywhere else, this would be called libel

Government

- The minute you read something you can't understand, you can almost be sure it was drawn up by a lawyer.
  Will Rogers (1879-1935)

- Has the most to lose
  - The ultimate risk manager
- Mistakes are costly
  - Action
  - Inaction

Some General Common Approaches

- Risk Management
- Cost Effectiveness
- Reasonableness
- Technical neutrality
- Business needs driven

Government Regulation

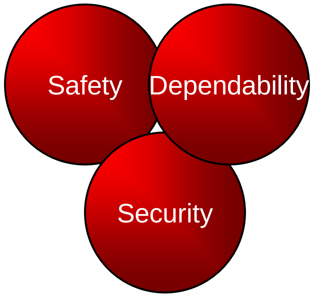
- Regulatory Compliance
  - Industry Specific: FAA, FDA, NRC, Financial Services
  - Industry non-specific: FTC, Sarbanes-Oxley, CA SB 1386
- Reactive in nature
  - Driven to “fix” the market
- Often derived from industry standards
- Generally emotionally driven: Political debate

An Example: CA SB 1386

- On the surface, it seems like a good idea
  - Businesses must warn consumers if their private data is compromised
- But upon further reflection,
  - The bill tries to secure the fundamentally unsecurable: identifiers
  - Now diverts resources away from solving the real problem: secure, authenticated transactions
  - Gives the illusion of progress

Summary

- The “system” has many areas of unaccountable activities
- Socially, we’re increasingly dependent upon information technology, systems, and services
- Dependency requires us to develop, deploy, and maintain safe, dependable, and secure critical infrastructure
- We can do it… but we haven’t so far
- Government can both help and hurt
- “There is no conflict between liberty and safety. We will have both or neither.”
  - Ramsey Clark



Safety

Dependability

Security

Panel topic area ideas

- Can American Free Enterprise deliver safe, dependable, secure consumer infrastructure?
  - In the last 25 years, has it?
- Do we want government to change the market?
  - Regulation?
  - Product liability?
  - Other ways?
- How do we hold decision makers accountable for their actions? Should we?
- How do we better match risk and reward?
- What engineering standards do we want?
- What accountability do we need to meet the public's interest in safe, secure, and dependable information infrastructure?

"Technological progress is like an axe in the hands of a pathological criminal."
Albert Einstein (1879-1955)

About Mike Jerbic, CISSP, PMP

Mike Jerbic, the firm’s principal consultant is an information security professional with 10 years of experience in engineering, management, and development of Hewlett-Packard enterprise security products. He directed the utility services program for HP’s disaster recovery product “Data Protector,” and the security, systems management, repository, and networking program for “E-Speak,” a distributed a Web Services framework. Prior to that he managed HP’s UNIX operating system’s kernel and commands security project for seven years where he led the release of Common Data Security Architecture, Pluggable Authentication, Trusted NIS+, all the while improving quality and eliminating legacy UNIX vulnerabilities. Before becoming a manager, he served as developer, and later architect, of PC storage systems at HP. His combination of development and management experiences make him a pragmatic strategist.

Active in his profession, Mike contributes his time and expertise to a number of professional organizations including:

- Chairman, The Open Group Security Forum
- The American Bar Association’s Information Security Committee
- San Francisco Bay Infragard
- The Silicon Valley Chapter of the Project Management Institute

About Trusted Systems Consulting Group

- Who we are
  Trusted Systems Consulting Group consists of a network of experienced enterprise systems information security professionals with engineering, management, and legal experience in the high tech industry. We have deep experience in the development and deployment of enterprise platform, middleware, application, and business continuity security products, having worked with major accounts in many industries solving digital signature, information integrity, and assurance problems. We focus on solving business problems, taking a broad view of the client's security needs and current system to identify pragmatic, cost-effective solutions. This approach minimizes business disruption, solves the client's security problems for the long term, and minimizes overall cost of ownership.

- Our Services
  - Policy assessment and development
  - IT project development services including implementation, and project management
  - Product development services including engineering, product management, project management, and program management
  - Operations analysis and optimization
  - Training and awareness building
  - Regulatory Compliance consulting

- We want to work with you. To contact us:
  - Mjerbic@trustedsystemsconsulting.com
  - 408.257.1648