TRIPWIRE

An IT Safety Index: Measuring Capabilities for Repeatable Builds and Remediation (And Why We're So Bad At It…)

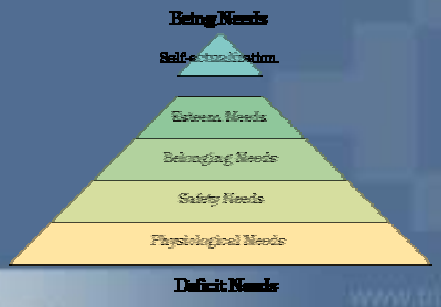
Gene Kim

CTO, Tripwire, Inc.

December 12, 2001

First, Who is Maslow?

- Psychologist who created "hierarchy of needs" in 1950s
- Air >> Water >> Food >> Sex >> Happiness



Agenda

- Common IT pains and root causes
  - Symptoms
  - Historical context
  - Problem restatement
- An IT Safety Index
- Historical context
  - Forces for change
  - What is going wrong

TRIPWIRE

Why Is IT In So Much Pain?

- "When something goes wrong, they usually point to the closest piece of IT…"
- IT mishaps are frequent and costly
  - Large surprises
  - Large remediation efforts
  - Enormous consequences of security breaches
  - Rebuilding servers more than we like to admit

TRIPWIRE

What Causes IT Pain

- Common IT maladies
  - Constant "fix/break" cycles
  - Loss of repeatable builds
  - Lack of ability to detect change
- Consequences are easier to spot…
  - Microsoft DNS outage – 22 hours to remediate
  - Egghead.com – six weeks to verify damage
  - Worms! Worms! Worms!

TRIPWIRE

No Perfect Change Control Board

- Mainframe era: Change control was imperfect
- Post-mainframe: Problems are magnified thousand-fold – many claim loss of most production controls
- Mainframes had several advantages:
  - Experienced and highly skilled technicians
  - Centralized control
  - MIS lifecycle

TRIPWIRE

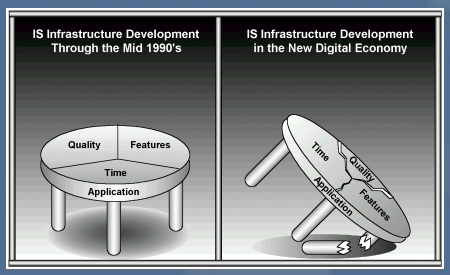
Capacity Expansion Too Easy?

- Entire new class of infrastructure created:
  - Web server farms
  - File servers
  - Appliances
- Repeatable builds often lost long ago…
  - It's like a plane that has lost its ability to land and take off – we can merely refuel it in mid-air and attach new engines.
- Attacker/defender mismatches
  - 4-5 orders of magnitude differences in…
  - Capital, lifecycle times, …

TRIPWIRE

Accelerating Lifecycles

- Classic IT and software engineering lifecycles: Time, Resources, Quality
- "IS professionals face demands for new applications with more functionality that must be delivered to distressingly compressed time schedules." *Aberdeen.*



Source: Aberdeen

TRIPWIRE

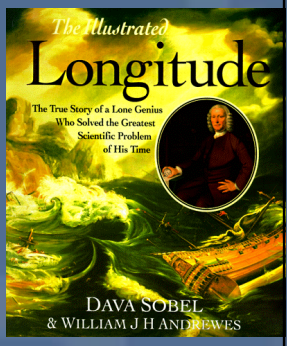
No Server Undo: We can add, but not subtract

- Software installation is an irreversible function
  - "Give me root on your favorite Linux machine – I want to make it run better…"
  - "Let me borrow your Windows 2000 laptop for a day. I want to install some software."
- Would you be able to undo the damage?
  - How is this any different than recovering from an attack?
  - This is science?
- We can add, but we can't subtract – best we can do is start over, and add quickly…

TRIPWIRE

The Story of Longitude

- Snapshot of 1700 Shipping:
  - Approx. 300 ships a year were crossing the Atlantic Ocean
  - One Spanish galleon carried a significant percentage of English GNP
  - Navigational tools made each transit risky
  - Safe passage more luck than skill. Why?



TRIPWIRE

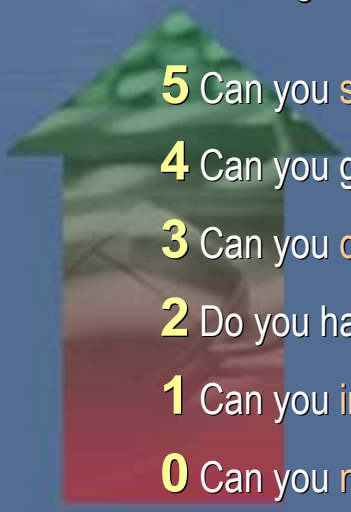
Another Clue

- Abandonment rate of many Intrusion Detection technologies is 80%
- Why?
- Where else can we see these patterns?

TRIPWIRE

The IT Safety Index

Where does an organization fit? (Kim/Spafford)



5 Can you scale economically?

4 Can you get early warning of threats?

3 Can you detect changes?

2 Do you have repeatable builds?

1 Can you inventory critical biz processes?

0 Can you name a critical biz process?

TRIPWIRE

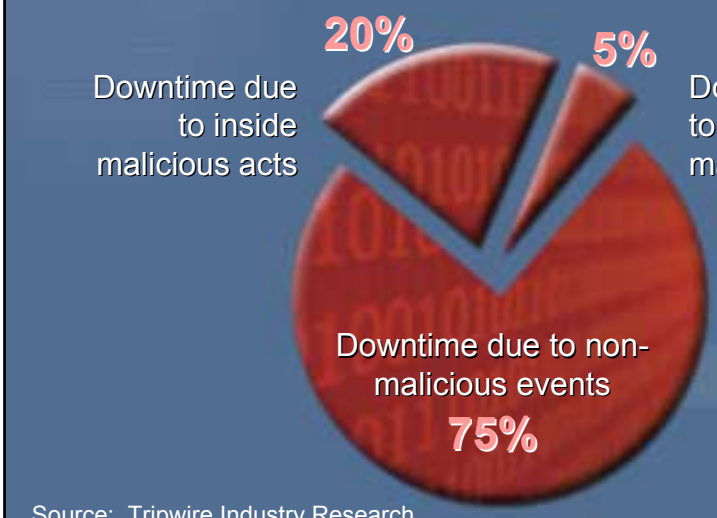
Historical baggage of change control

- Change is risk…
- So, in 1980s, MIS departments always said no
- Created the opportunity for modern computing environment
  - Change happens fast
  - Operational art of data centers has disappeared
  - Problems of the 1960s – 1970s have returned
  - So, IT is in a lot of pain

Technology and Economic Forces

- "Cheap and crappy" almost always beats "Expensive and better"
- Innovator's Dilemma: rate of technology adoption accelerating
- Combined with "computing at the speed of business mentality," we end up deploying more infrastructure that is plagued with problems

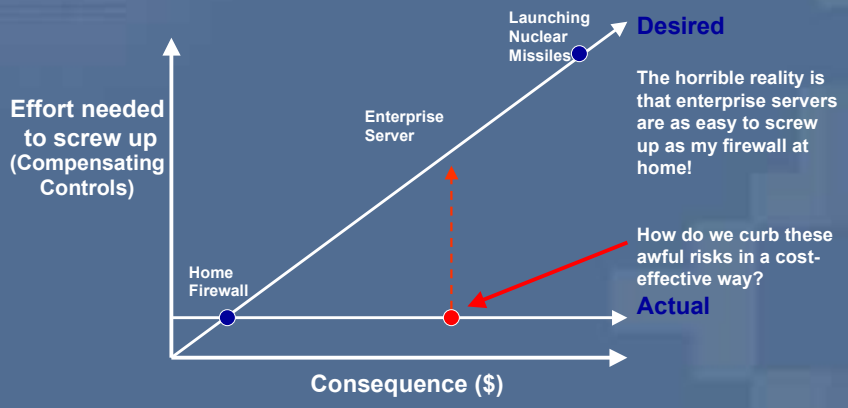
Causes of System and Network Downtime



Source: Tripwire Industry Research

TRIPWIRE

Compensating Controls



TRIPWIRE

Key Pains

- IT infrastructure is operationally dangerous – small mistakes often have catastrophic consequences
- IT operations often running with no safety net
- Change control remains an imperfect art
- Security "symptoms" often because of loss of repeatable builds, and inability to maintain control

TRIPWIRE

Closing Thoughts

- Smart people have been using Tripwire for almost ten years – I want to understand why…
- Many IT problems get blamed on security – in reality, they hinge on stability and safety
- Security often "moving deck chairs on the Titanic" – maybe it's time to get a new boat?
- Fix/break cycles happen even in top-tier IT shops
- Keep moving responsibility and accountability upstream

TRIPWIRE

Longitude

- If you want a copy of any of these…
  1. Book: *Longitude*
  2. Poster: *Servers Under Siege: A Day in the Life of an IT Defender*
  3. *This PowerPoint presentation*
- …leave a business card or email me!
  genek@tripwire.com

TRIPWIRE