Auditable Security Controls Of Best In Class Security and IT Operations Organizations:

*What Do They Do And How Do They Do It?*

*Gene Kim, CTO, Tripwire, Inc.*

*September 2004*
Surprising Executive Allegations

- We have heard some very surprising things in the 30 Practitioner Roundtables we’ve hosted in the last four years
  - Control and security are not possible
  - Change management is bureaucratic, slows work down, decreases productivity, and is overly burdensome
  - My business demands are so high in my environment is so high, that the management of change is not possible
  - I can sustainably achieve my security objectives without repeatable, verifiable IT operational processes

- Really? Why do they believe these things?
  - Is there anything we can do to change their belief systems?

TRIPWIRE
Best in class Ops and Security organizations have:

- Highest server/sysadmin ratios
- Lowest Mean Time To Repair (MTTR)
- Highest Mean Time Between Failures (MTBF)
- Earliest integration of Security into Ops lifecycle
Talking Points

- What is common among the high-performing IT organizations?
  - What are their beliefs?
  - Why do they hold these beliefs?
  - What behaviors and characteristics do they exhibit?
- What are the key differences between the high- and low-performing IT organizations?
  - Patch management, management scorecards, IT outsourcing
- How do organizations transform from a low- to high-performing IT organization?
  - Visible Ops methodology
  - Process area metrics
- The VEESC Benchmarking Study (Valuing the Effective, Efficiency and Security of IT Controls)
  - The hypothesis and methodology
  - Our call to action!
History of IT Operations and Security Research

- Began studying high-performing IT operations and security organizations in 2000, to understand their processes and implementations. These organizations exhibited:
  - Highest availability
  - Shortest MTTR
  - Lowest IT cost profiles
  - Least amount of time spent on unplanned work
  - Best integration of security into operational processes

- Now working with IT Process Institute, CMU’s Software Engineering Institute and SANS to understand how high performing organizations work manage IT to achieve business objectives
  - Functional roles span: IT Operations, Audit, Security, Management, Governance, etc…
  - 04/2003: Co-chaired SANS Auditable Security Controls That Work
  - 10/2003: Co-Chaired SEI Best in Class Security and Operations Roundtable
  - 10/2004 (in planning): Co-Chairing SANS Defining IT Operational Training Curriculum
Common Traits Of The Highest Performers

- **Culture of change management**
  - Integration of IT operations and security processes via problem management and change management processes
  - Processes that serve both organizational needs, as well as business objectives
  - Highest rate of effective change (approved changes, change success rate)

- **Culture of causality**
  - Highest service levels (MTTR, MTBF)
  - Highest first fix rate (unneeded rework)

- **Culture of compliance and continual reduction of operational variance**
  - Production configurations
  - Highest level of pre-production staffing
  - Effective pre-production controls
  - Effective pairing of preventive and detective controls
Causal Factors of IT Downtime

- Operator Error: 60%
- System Outages: 20%
- Application Failure: 20%
- Security Related: 5%
- Non-Security Related: 15%

Source: IDC, 2004
All the high-performers had self-derived the same way of working

- Culture of change management
- Culture of causality
- Culture of compliance and desire to continually reduce variance
Areas of Pain Identified by High Performing Organizations

- Volume of patches and patch management
  - Low performing: Adhoc, chaotic, urgent, disruptive; increase in unplanned work
  - High performing: Planned, predictable, just another change --> higher change success rate

- Proliferation of “scorecards” and other measurement, assessment instruments
  - Low Performing: Look to external sources, authorities; adopt scorecard du jour
  - High Performing: Have defined their own performance characteristics; can demonstrate traceability to other instruments

- Managing outsourced IT services
  - Transfer risk; out of sight; then unable to control
  - Manage like any other business unit or project; understand unique challenges; develop more bullet proof service level agreement
The absence of explicit articulation of current state and desired state obscures amount of pain
  – “It doesn’t hurt enough yet; don’t know that there is an alternative.”

A culturally embedded belief that control is not possible
  – Abdication of responsibility – “throw up my hands”

A system that rewards and reinforces personal heroics, instead of repeatable, predictable discipline
  – “What is overlooked is that if one person can save the entire boat, one person can probably sink it, too.”
Common Root Causes - 2

- The argument that IT ops and security are different (than other business investments or projects)
  - A common belief is that ongoing security can exist outside the scope of IT operations.

- The continual desire for a technical solution
  - Technology is easier to justify and implement than people and process improvements
Visible Ops: Four Steps To Build An Effective Change Management Process

- Each of the four Visible Ops steps is:
  - A finite project: not a ISO 9001 initiative or a vague 5-year vision
  - Catalytic: returns more resources to the organization than it consumes, fueling the next steps
  - Sustaining: process stays in place, even when the initial force behind it disappears
  - Auditable: supports factual reporting and attestation to process adherence and consistency
  - Ordered: must be done in the specified order to achieve the above

- Model based on five years studying high-performing IT Ops and Security organizations
- Visible Ops has been donated to the ITPI
Visible Ops: Four Steps To Build An Effective Change Management Process

Phase 1: Electrify Fence, Modify First Response
- Tripwire enforces the change process.
- Tripwire rules out change as early as possible in the repair cycle.

Phase 2: Catch and Release, Find Fragile Artifacts
- Tripwire protects fragile artifacts.
- Tripwire enforces change freeze and prevents configuration drift.

Phase 3: Establish Repeatable Build Library
- Tripwire captures known good state in preproduction.
- Tripwire captures production changes that need to be baked into the build.

Phase 4: Continually improve
- Tripwire detects change, which all process areas hinge upon.

Tripwire enforces the change process,Tripwire rules out change as early as possible in the repair cycle.Tripwire protects fragile artifacts.Tripwire enforces change freeze and prevents configuration drift.
Which Metric Do You Want To Improve?

- **Release**
  - Time to provision known good build
  - # turns to a known good build
  - Shelf life of build
  - % of systems that match known good build
  - % of builds that have security sign-off
  - # of fast-tracked builds
  - Ratio of release engineers to sysadmins

- **Controls**
  - # of changes authorized per week
  - # of actual changes made per week
  - Change success rate
  - # of emergency changes
  - # of service-affecting outages
  - # of “special” changes
  - # of “business as usual” changes
  - Change management overhead
  - Configuration variance

- **Resolution**
  - MTTR, MTBF
  - % of time spent on unplanned work
Thought Experiment

What is more desirable?

- 1000 servers, configured identically, but configured insecurely
- 1000 servers, configured randomly, but 20% configured in a secure manner

Most high performing organizations would choose the first. Why?

Ability to systematically change all configurations, ability to defeat entropy, ability to maintain any desired state…
The Information Technology Process Initiative (ITPI), a not for profit organization, is engaged in three principle areas of activity, Research, Benchmarking and the Development of prescriptive guidance for practitioners and business executives.

The ITPI has collaboration agreements in place with research organizations such as The University of Oregon Decision Sciences program and The Software Engineering Institute at Carnegie Mellon University.

We are currently working to create prescriptive guidance that solves the common objectives of IT Security, Corporate Governance, Audit and Operations.

Through Research, Development and Benchmarking the ITPI creates powerful measurement tools, prescriptive adoption methods and control metrics to facilitate management by fact.

http://www.itpi.org
Hypotheses

- That there is a low cost of quality for attaining high-performing and best-in-class characteristics
  - For instance, to achieve high availability, you can achieve by repeatable processes or controls, or by throwing enough resources at the problem (ad hoc)
  - In the two cases, how much does it cost to increase availability by 1%?
  - Show that processes allow linear improvement, while ad hoc creates exponential cost
- That the thinking processes of high-performance IT operations management can be quantitatively and qualitatively correlated
Hypotheses

- That within the five BS 15000 process areas, the release, controls and resolution are dominant
  - The three process areas create leading indicators (exogenous), while the remaining process areas create trailing indicators (endogenous)

- Candidate controls for correlation (and causation)
  - Change management
  - Release and configuration management (inventory)
  - Incident and problem management
  - Service level and availability management
  - Service catalog
  - Intrusion detection and access controls
Summary

- Visible Ops is the result of years of studying high-performing IT operations and security organizations in conjunction with the ITPI.
- Transformations are possible and repeatable.
- Visible Ops shows how to make these transformations in just four, achievable steps.

- Gene Kim: genek@tripwire.com