CERT PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Change Management: The Security 'X' Factor

Key Message: In a recent survey of organizations' security posture, one factor separated high performers from the rest of the pack: change management.

Executive Summary

In a recent survey of organizations conducted by the IT Process Institute, one factor separated all of the high performers from the medium and low performers. This "X" factor had nothing to do with complex access controls, number of deployed security products, or any other traditional metric. Instead, it was something many organizations view as an operations issue rather than a security issue: change management.

In this podcast, Tripwire CTO and IT Process Institute co-founder Gene Kim discusses the survey's findings, why change management turned out to be such a competitive differentiator, and how organizations can harness the power of change management to achieve optimal security.

PART 1: THE STUDY

Background

Since 1999, the IT Process Institute has been studying IT operations and security organizations. Several organizations were designated as "high performers." Organizational size and industry varied widely - so what was the common thread?

Initial indicators of high performance included:

- best service levels as measured by MTTR (mean time to repair) and MTBF (mean time between failures)
- best security as measured by earliest and most consistent integration of security into the IT operations life cycle
- best posture of compliance as measured by fewest number of repeat audit findings and fewest number of staff dedicated to compliance activities
- most efficient, as measured by high server-to-system-administrator ratios and low amounts of unplanned work

The Visible Ops project started as a way to find out what these 11 identified "high-performing" organizations were doing differently. The project found:

- a culture of change management
- a culture of causality

Disaster and other continuity-interrupting events had brought each organization independently to this point. Remember: "Behind every FAA regulation is an airline crash."

The Performance Gap

In 2004, ITPI started the IT Performance Control Study to verify the Visible Ops findings. The study benchmarked 98 organizations and used six IT Infrastructure Library ITIL process areas as the basis for extracting 25 of the most meaningful control measures.

Predicted performance difference between high and low performers: 2X.
Actual performance difference: 5X to 8X.

Specifically, high performers:

- Did 8 times as many projects
- Managed 6 times as many applications
- Implemented 7 to 14 times as many changes
- Had one-half the change failure rate
- Had one-quarter the first-fix failure rate
- Had five times higher server-to-system-administrator ratios
- Had budgets three times higher

There are 2 possible explanations:

1.) High performers are more successful because they have more money.

2.) High performers are doing the two IT jobs well: delivering new projects to the business; and operating and maintaining existing projects and assets. So they are able to increase funding due to high performance; low performers can't do either task well.

Just as with performance, the security difference between high performers and medium or low performers was 5X to 8X.

What Made the Difference?

Of the 6 ITIL process areas and 63 ITIL controls benchmarked by the study, 2 stood out as differentiators:

1.) Do you monitor systems for unauthorized change?

2.) Do you have defined consequences for intentional, unauthorized change?

EVERY high performer answered "Yes" to these questions.
NO medium or low performer answered "Yes" to these questions.

Additionally, setting the tone from the top is extremely important. The only acceptable number of unauthorized changes is zero, and this should be made clear to all employees from the CEO on down.

PART 2: TAKING ACTION

Change Management Catalysts

To keep the organization on track, publish 3 things:

1.) All scheduled authorized changes.

2.) All unauthorized changes.

3.) The consequences and ramifications to any person who made any unauthorized changes.

This is similar to an audit-based approach.

Remember: Trust is not a control. Hope is not a strategy.

Look at every unplanned outage. Chances are, behind every unplanned outage is a failure in the change control process.

Why Is Change Management So Important to Security?

Looking back in history, there were 3 keys to security:

1.) access controls
2.) change controls
3.) business continuity (ability to restore service)

The study shows you don't get the breakthrough in performance until you tackle change. This confirms deeply held intuitions of practitioners who operated decades ago.

If you don't have control over change, you really don't have control at all.

Implementing Change Management

Access controls are typically viewed as a security issue, and security departments often have complete control over access (issuing and revoking entitlements, as well as provisioning).

The same is not true for change management. Security-related job descriptions don't emphasize it.

In high-performing organizations:

1.) There is always a champion for change management.

2.) Security owns the prosecution of unauthorized changes. In other words, if an unauthorized change is made, and IT operations doesn't prosecute it to completion, it becomes security's responsibility. This is not something security needs to ask for - it's part of the culture.

Implementing change management can provide the evidence that security is helping day-to-day operations (more projects, more changes, better change success rates, etc.).

PART 3: OVERCOMING HURDLES

Revamping Change Management's Image

Biggest hurdle: the perception that change management is bureaucratic, slows things down, sucks the will to live out of employees.

This is not the case!

More projects get done.
More changes get made.
There is less unplanned work due to failed changes.

There are some other common misperceptions to overcome:

1.) "We don't want to put our creative people in a cage."
Counterargument: Sometimes creativity (such as on a production line) is inappropriate.

2.) "Our people are too highly paid for us to micromanage."
Counterargument: With something as mission critical as IT, the worst thing that can happen is not to have control.

Most importantly, management needs to determine what to do with a nonconforming employee who keeps making unauthorized changes. Maybe you put him in a role where he can't make changes anymore. Don't fire him, but place

him in a role more suited to his temperament.

Benchmark Yourself

If your change management process isn't working, look for:

- Do you monitor systems for unauthorized change?
- Do you have defined consequences for intentional unauthorized change?
- Is the tone set at the top of the organization?
- Are you enforcing your change management process, or is it just a binder on a shelf somewhere?

To confirm that change management is working, look for:

- Fewer unplanned outages
- Reduction in mean time to repair
- Increase in the percentage of changes that are on-time and work right the first time

High performers have change success rates of more than 90%. Low performers may have success rates as low as 50% or 60%.

Resources

Additional Podcasts and Interviews with Gene Kim

Purdue CERIAS Security Seminar Series:
http://www.cerias.purdue.edu/news_and_events/events/security_seminar/details.php?uid=ve3d844b8277lei2sgb9io1d8c@google.com

ZDNet: http://blogs.zdnet.com/threatchaos/?p=395

IT World: http://www.itworld.com/Man/2677/transcript_genekim_geer060906/pfindex.html

CSO Magazine: http://www.csoonline.com/podcasts/Tripwire_Aug06_CSO_Kim.html

References

Bartholomew, Doug. "Better Controls Yield Better Performance." *Baseline Magazine*, August 28, 2006. http://www.baselinemag.com/article2/0,1397,2009454,00.asp

Behr, Kevin; Kim, Gene; & Spafford, George. *Visible Ops Handbook: Starting ITIL in Four Practical Steps*. IT Process Institute, 2004. Introductory and ordering information is available at http://www.itpi.org.

Kim, Gene, et al. *IT Controls Performance Study: Identification of foundational controls that have the greatest impact on IT operations, security, and audit performance measures*. IT Process Institute, 2006. Ordering information is available at http://www.itpi.org.

Kim, Gene, et al. "Prioritizing IT Controls for Effective, Measurable Security." IT Process Institute, November 2006. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/deployment/577.html

The Institute of Internal Auditors. *Global Technology Audit Guides: Change and Patch Management Controls: Critical for Organizational Success*. July 2005. http://www.theiia.org/index.cfm?doc_id=5167

Supporting Materials

Information Technology Governance Institute. *COBIT 4.0 Control Objectives for Information and related Technology*. ITGI, 2005. http://www.itgi.org and http://www.isaca.org.

IT Infrastructure Library. *Security Management*. Office of Government Commerce, Crown, 1999.

IT Infrastructure Library. *Service Support*. Office of Government Commerce, Crown, 2000.

IT Infrastructure Library. *Service Delivery*. Office of Government Commerce, Crown, 2001.

International Organization for Standardization. *Information technology - Security management* (ISO/IEC 20000-1:2005(E)), First edition, December 15, 2005. *Part 2: Code of practice* (ISO/IEC 20000-2:2005(E)), December 15, 2005.
