CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Connecting the Dots between IT Operations and Security

Key Message: High performing organizations effectively integrate information security controls into mainstream IT operational processes.

Executive Summary

Aligning information security with IT operations to help meet business objectives in a demonstrable way is easy to say and hard to do. Based on several years of benchmark research, there are a set of proven, sound practices that allow enterprise IT operations and security teams to effectively operate and maintain production systems and meet security-based compliance requirements while providing new business-driven services [Kim 08].

In this podcast, Gene Kim, CTO for Tripwire and a founder of the IT Process Institute, discusses specific steps for integrating information security and IT operations based on benchmark results from high performing organizations. This work is described in ITPI's recently published book *Visible Ops Security: Achieving Common Security Objectives in Four Practical Steps*.

PART 1: THE DISCONNECTS, AND WHY BUSINESS LEADERS SHOULD CARE

Background

Since Gene's first podcast (Change Management: The Security 'X' Factor), he has been involved in a substantial benchmarking effort with the IT Process Institute titled "IT Controls Performance Study." Based on data from over 330 IT organizations, the study identifies the foundational controls that have the greatest impact on IT operations, security, and audit performance.

This study provided insight and data for a recent ITPI publication titled *Visible Ops Security: Achieving Common Security Objectives in Four Practical Steps*. We discuss key findings from this work (SVO) in this podcast.

The Disconnect Between IT Operations and Security

IT Operations (IT) can make life difficult for Information Security (IS), for example by deploying an insecure component into production. This could result from:

- no security standards to start with
- lack of documented or communicated security standards
- software forced into production due to time-to-market pressures before security could be addressed
- IS doesn't understand all of the projects that IT is managing
- IT's focus on keeping systems up and running (required to meet tough availability objectives) causing security to be moved to the backburner.

When IT Operations can't achieve their own goals, they certainly can’t achieve security goals.

IS can sometimes make life more difficult for IT by unintentionally creating controls that add bureaucracy and overhead. This can create a backlog and delays if security is the last step in the review cycle before software is scheduled to go into production.

IS involvement, in this case, can hold up critical IT projects.

The Disconnect Calls for Business Leader Attention

IT and IS are getting in each other's way while both fail to achieve their objectives:

IT isn't providing a reliable, stable, secure IT production environment.

IS isn't safeguarding the business' goals, objectives, and information. This can include:

- poor performance on security breaches
- non-compliance with laws and regulations
- lack of identification and creation of controls that reduce business risk.

Making Security a Business Issue – for IS and for Business Leaders

Business leaders need to specify information security objectives from a business perspective. These may include:

- quickly find and correct security breaches, ideally before users and customers are impacted
- be active, engaged custodians to prevent the loss of confidential or personally identifiable information
- help create a stable and secure IT infrastructure that provides reliable IT services that are critical for business operations
- make sure the business is in compliance with laws and regulations, such as the Payment Card Industry standard, HIPAA (Health Insurance Portability and Accountability Act), and SOX-404 (Sarbanes Oxley Act of 2002) – so that risks of public disclosure for non-compliance are minimized.

Security Is About More Than Compliance

IS is often perceived as irrelevant, bureaucratic, not aligned with the business, and too focused on technical details.

It is important to understand what IS looks like when it is providing value to the organization, such as when it enables global supply chain partnerships. The next section describes what high performing IT and IS organizations do to add business value.

PART 2: BENCHMARKING AND SITUATIONAL AWARENESS

Key Roles for IT and IS

There are two primary roles:

- operate and maintain production systems to meet business and compliance requirements
- have sufficient capacity and capability to provide new business-driven services

Characteristics of High Performing IS Organizations

As part of the IT Controls Performance Study, Gene's research team identified the following characteristics for high performing IS organizations:

- aligned with the business, understanding business needs and requirements
- plugged into the IT production environment and day-to-day IT processes
- able to integrate IS tasks effectively into mainstream IT, software development, application development, release management, and project management processes
- viewed as a critical stakeholder by these organizations (listed in the previous bullet)
    - if IS is not available for meetings, the meeting is delayed or rescheduled
- effective in scoping and prioritizing what needs to be done
- people savvy, as evidenced by their interest in adding value and helping others achieve their objectives while

simultaneously achieving IS objectives.

These characteristics were evidenced in organizations of all sizes across sectors.

Gaining Situational Awareness

The first phase in Visible Ops Security (Stabilize the Patient and Get Plugged into Production) stresses the importance of IS being aware of its business and IT environment. This includes getting plugged into production and becoming a key player in how the organization operates – identifying the critical stakeholders and major projects.

Getting plugged into production involves making sure IS is integrated into the change management process – managing by fact, ensuring all changes are authorized, and adding value to the process.

IS helps create the right tone at the top by making sure IT management takes decisive action when people make unauthorized changes.

Through these steps, IS helps the organization substantiate the effectiveness of controls for audit and compliance activities.

So situational awareness means:

- getting an accurate handle on the production environment and what's coming into production (the pipeline)
- understanding the security threat and risk landscape and communicating this

The remaining steps in SVO Phase 1 include:

- plugging into access management processes to help ensure that IT can trace all privileged accounts to a real person and that approvals are appropriately authorized
- integrating security incident response procedures into IT incident management processes. The IT 24x7 help desk processes should be used for security incidents.

The idea throughout SVO is to ensure that security controls are fully integrated into mainstream IT operational processes.

PART 3: RISK-BASED SCOPING, UPSTREAM INVOLVEMENT, AND MEANINGFUL METRICS

Addressing Security from a Risk Perspective

During the early days of SOX-404 compliance efforts, IT was spending an excessive amount of time testing controls that ended up not contributing to accurate financial statements. This was a key lesson learned.

The Institute of Internal Auditors GAIT project helped codify how to appropriately scope the IT-relevant portions of SOX.

Visible Ops Security Phase 2 (Find Business Risks and Fix Fragile Artifacts) reflects what was learned here about using risk as the basis for control ranking, prioritization, and selection.

The important message here is to focus on the few controls that really matter, using knowledge of key business processes to identify where they are dependent on critical IT functionality. Then IT can focus on making sure these controls are working effectively.

The Concept of Fragile Artifacts

Fragile artifacts are pieces of IT infrastructure that are prone to break, have high business outage costs, and/or have

high mean time to repair. Fragile means operationally fragile, as well as fragile with respect to demonstrating compliance or meeting internal control objectives for financial reporting.

Fragile is synonymous with "risky," so it is a useful concept in helping prioritize where IS and IT should focus their attention.

Implement Development and Release Controls

SVO Phase 3 describes how to integrate IS into upstream development processes to ensure that software that goes into production is secure and of high quality.

IS needs to work with project management to, among other things, help codify security standards, help train development staff on them, create a library of secure, reusable code, and integrate with the quality assurance function to help test for information security risks.

It is important for IS to have an informal relationship with internal audit (IA) as well, given IA's perspective on organizational risks. This collaboration can result in fewer audit findings, few repeat audit findings, and less time addressing audit findings.

Measuring Progress and Outcomes

Each phase of SVO describes outcome measures and metrics that are useful for demonstrating progress and results. Some of Gene's favorites include:

For IS:

- percent of security breaches that result in a loss event - high performers are able to fix a breach quickly before it becomes a catastrophe
- percent of security breaches that are detected by an automated control - by using automated controls, high performers often detect breaches in minutes rather than weeks or months
- percent of the organization's time that is spent preparing for audits
- number of repeat audit findings

For IT:

- percent of an organization's time spent on unplanned work
- roject due date performance
- percent of changes that work the first time with the desired outcomes (change success rate)
- first fix rate (ability to fix a problem the first time)

The IT measures are further elaborated in *The Visible Ops Handbook: Starting ITIL in 4 Practical Steps*, published in 2004.

Resources

[Kim 07] Kim, Gene; Love, Paul; Spafford, George. Visible Ops Security: Achieving Common Security Objectives in Four Practical Steps. IT Process Institute, 2008.

"An Introduction to Security Visible Ops with Gene Kim." Tripwire Webcast.

Behr, Kevin; Kim, Gene; Spafford, George. The Visible Ops Handbook: Starting ITIL in 4 Practical Steps. IT Process Institute, 2004.

The IT Process Institute