DITY™ Weekly Newsletter
itSM Solutions®
IT Experience. Practical Solutions
The workable, practical guide to Do IT Yourself Vol. 4.40 . October 7, 2008

The Importance of ITIL to (Am I Reading This Right?) ... Security??

By Scott Crawford
Research Director - Enterprise Management Associates

What is one of the most important foundations of IT security management? Simple: it's ITIL. That's probably not the answer you would expect from a security professional. When asked this question, it seems people usually expect the answer to point to technologies for IT defense, or—to the extent they are relevant at all—guidance such as security-specific ISO or NIST standards, or compliance mandates such as the Payment Card Industry (PCI) Data Security Standard.

But I don't, because I have actually been a Chief Information Security Officer for an international organization, and I know from experience that security is not just a process, but one of the most contentious intersections of people and culture with technology.

So where does IT look for best practices in aligning people, process and technology? To the principles of IT Service Management—and those who excel there do many of the same things that are essential to assuring reliable security. The fact that neither IT managers nor security professionals recognize this often enough is a direct cause of the poor state of security in so many organizations worldwide.

In this article, we'll take a look at some specific examples of how ITIL is critical to security—and yes, you read that correctly.

But first, we'll first have to explode an ITIL myth.

"ITIL doesn't really speak to security...does it?"

Anyone who says that ITIL is irrelevant to security because it is "light" on the subject, simply does not get it. The fact that versions of ITIL (at least before v3) either gave a broad brush to security specifics or pointed instead toward other guidance such as ISO 17799 and its descendants, is not relevant to the importance of ITIL and ITSM to security.

Rather, the fact that best practices in IT Service Management point the way to defining, implementing, monitoring and assuring repeatable IT management objectives and processes is the key.

Consider for a moment the relevance of these ITIL domains to **Security Management:**

- In **Service Support:**
  - **Configuration and Change Management** determine whether IT presents a solid defense against security threats or vulnerabilities that expose the enterprise to today's more sophisticated attacks. When vulnerabilities are detected, Configuration and Change Management can assure the reliable and repeatable deployment of remediation, and help identify the highest priority risks.
  - **Release Management** often centers on the deployment of reliable, quality-tested IT resources. Considering how many of today's attacks target application environments, the failure to incorporate security in the development and release of IT applications and services can be a major gap in defense.
  - **Incident and Problem Management** are central not only to accurately identifying cases where security issues are the root cause of an incident or problem, but effective response to security events. Reliable and

repeatable processes for incident response can mean the difference between a threat contained and mitigated, or chaos that, in the worst cases, can lead to panic among business stakeholders and IT professionals alike. Informed security incident response is also essential to collecting forensic critical to the success of a personnel or legal action.

- **Service Desk and Service Request Management** is not only a focus of IT Service Management, it is often a nexus of one of the key process disciplines in IT security: identity and **Access Management**. Requests for user provisioning are often referred to the **Service Desk** for action. Provisioning processes often include management reviews and evaluations of appropriate entitlements. Once granted, access control becomes a first line of defense in separating authorized access from threats.

Stating the core values of information security in the oft-quoted terms of Confidentiality, Integrity and Availability (CIA) further highlights the relevance of security to **Service Delivery** domains of **Capacity and Availability Management**. Organizations may also look to **Service Level Agreements** (particularly **Operating Level Agreements** with external service providers) to define terms of acceptable security incident and event recognition and response, and may measure **Service Level Management** performance in meeting these objectives as a key security metric.

The increasing importance of incorporating security throughout the lifecycle of IT services calls attention to security in each of the four phases of **Service Strategy**, **Design**, **Transition** and **Operation** articulated by ITIL v3, while the ongoing assessment and improvement of security plays a role in **Continual Service Improvement**. This has become particularly pronounced in managing the increasing number of threats that target modern web applications, where security throughout the Software Development Lifecycle (SDLC) has become essential to securing applications that are often both unique and dynamic.

ITIL as IT Risk Management

Viewing security in this light-and, conversely, ITIL in the context of security-highlights that security is itself part of the broad spectrum of IT risk management, where the definition of realistic objectives and repeatable management makes the difference between success in IT management and inefficient chaos that is itself a primary risk factor.

Recent research conducted by EMA has borne this out. In 2008, EMA surveyed over 200 global organizations about their IT security, risk and compliance management efforts. It asked them about the criticality of IT to their primary business objectives, such as maintaining a competitive edge through access to new markets, or to processes such as product manufacturing and supply chain optimization.

It asked them about their outcomes in terms of security events disruptive to IT performance, availability or information resource integrity, as well as incidents resulting in a data security breach. And it asked them about the management disciplines had the greatest impact on their outcomes.

What EMA found was that the highest performers consistently **define** management objectives and repeatable processes; they actually **implement** them; they **monitor** the real-world factors that affect these priorities; and they **respond** consistently to issues as they arise.

This becomes particularly evident in areas such as **Configuration** and **Change Management**. 94% of high performers define IT change processes, actually implement those processes, monitor adherence in the IT environment through technologies such as change audit and configuration management, and enforce consequences for deviations.

Not surprisingly these same high performers experienced about half the median number of disruptive security incidents as both medium and low performers. They also experienced lower rates of unplanned IT work, high rates of successful IT changes, greater numbers of IT projects delivered on time, within budget and with expected features, and high server-to-sysadmin ratios.

In other words, these high performers are not only more secure, they are more efficient—a critical factor in today's more cost-sensitive environment. Just ask any military veteran: better discipline leads not only to better security, but to improved reliability and greater efficiency as well.

SUMMARY

In the past, the message of ITIL was greeted by security professionals with a yawn at best, while the security values of ITIL were often overlooked or ignored outright by IT Service Management professionals who should have known better.

Today, businesses are finally beginning to wake up to the value of defining repeatable, reliable processes for managing IT risks and security events, and just what the values of ITIL and IT Service Management can mean to make security more realistic, more efficient—and more cost-effective—than ever before.