Marrying Security to Operations:

Honeymoon in the making or in-laws in the shadows?

By Chris Farrow

When IT administrators face day-to-day business concerns, security planning is usually at the top of a short list of priorities. But when the time comes to actually do something about IT security, spending on planning usually gives way to weightier, performance-based directives.

However, in an era when processes are making their way back into the mainstream—such as ITIL, BASEL II and ISO 17799, the choice on whether to invest in better security precautions or in something far more visible may no longer be the solitary choice of the business itself.

Welcome to the "Age of Compliance."

After years of exploits and misuse, government regulators throughout business are realizing that it's time for action. As long as business, defense and critical infrastructure industries continue to rely more on technology, trusting those businesses to make the right "safe" decisions on how to protect their customers' assets is slowly shifting to include "trust-but-verify" factors—also known as compliance mandates.

Business leaders often find themselves no longer able to feign ignorance on matters concerning security risk management. Conversely, as most IT security tools are reaction-based, finding technology to accomplish tasks associated with both security and operations may be more difficult than predicting the next virus. Moreover, administrators are not as eager to take advice from the security vendors, as the trend showed some three to five years ago. Given that IT security vendors include nearly a thousand commercial products and services, the operations people are starting to focus on strategies that can actually prevent problems, rather than create new ones to manage.

According to Gartner, more than 90 percent of all malicious activity is both known and dependent upon improperly configured environments.

According to Gartner, more than 90 percent of all malicious activity is both known and dependent upon improperly configured environments. But if administrators aren't willing to plan effective security contingency processes, the growing list of compliance mandates will ensure the job gets done.

Here are three factors to consider when considering the courtship between security and operations:

1. Technology addresses 10 percent of the problem. Without a process and the knowledge required to implement the process, no application will be effective in preventing or reducing risk.

   Look at the concept of Intrusion Prevention (IPS) technology, in which an incident must still occur before these types of tools actually do something (respond via e-mail, lock down a system, block further connections, etc.). Ironically, an event still has to take place—leaving intrusion "prevention" more aligned with intrusion "containment."

   Knowledge is the key to the success of blending security and operations. If you don't know your own environment, how will you know what to defend?

2. Managing risk means first identifying the state of a computing environment, and then ensuring that state is consistent with overall expectations. The question, in this case, is "Do you have enough information about where your assets are and what they're exposed to?"

   Gaining a better understanding of the IT environment simplifies the need to react to a mandate, or some other external control.

3. Nine times out of 10, vulnerabilities that are exploited are based on known problems—usually the result of poor configurations.

   A nine-to-one chance that administrators can prevent problems from ever happening means getting a dramatic lead on security risk management. Combine this factor with that described in #2 above, and administrators are still managing risks (and most of their potential security downfalls), by process-oriented means, rather than via a security point-solution, thereby achieving true Intrusion Prevention.

Following a more administrative approach to addressing potential risks, systems administrators should consider a configuration management database, or CMDB-driven data repository as the starting point. Administrators could actually prevent most of the risks to their IT infrastructures by first gaining a complete understanding of details associated with system settings and configuration controls at all points throughout the enterprise. Defining policy to which an organization builds a gold standard of operation without this critical step results in an ineffective, reactionary-based trend in enterprise IT security.

In a sense, you can't fix what you don't know is broken. However, you CAN plan for risks when you know what you have and how what's working before those risks are exploited.

Chris Farrow is the director of Configuresoft's Center for Policy & Compliance.