

## Sell the business on virtualization security

[http://searchSecurity.techtarget.com/magazineFeature/0,296894,sid14\\_gci1351978,00.html](http://searchSecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1351978,00.html)

by: Jack Phillips

Issue: [Apr 2009](#)

Virtualization has taken on a life of its own, sweeping across organizations of all sizes and shapes like a perfect antidote to all the inefficiencies in IT. Executive management has been rushing to inject this drug as quickly as possible, viewing all of the costs savings realized through virtualization as free. And in this economic environment, the pressure is particularly high to move quickly and ask questions about security later.

"Free" to a CFO or CEO means getting all the efficiencies without any commensurate risks. A few of the perceived freebies include faster time to market for new applications via "McServers," less physical space to house data centers and server farms, less power to cool and operate the data centers, faster and lower-cost disaster recovery.

But we in security know better. There are no free lunches in IT. Now that the antidote has taken effect in most organizations, some of the side effects are popping up. Things have moved so quickly that [IT security has struggled to define its role](#) in the new virtual world, to create the same relevance it has in the physical world.

IANS, an information security focused research firm, surveyed about 200 security executives last year on virtualization. Seventy-five percent use some form of virtualization software in their production environments, either at the client or server level. However, among those organizations polled, only five to ten percent of IT security teams were included in the decision to virtualize.

As virtualization deployments have grown in number, the implication of the survey results is clear: policies and architectures are not being updated to reflect the demands and constraints of a virtualized environment because [IT security wasn't included in the upfront planning and implementation](#). It's time to strategically insert your voice into those conversations.

This year more than ever, IT security's livelihood lies squarely in [how business owners perceive added security](#) will grow revenue or lower operational costs--it's that simple. Of course, this has always been true, but 2009 will be the ultimate test. Prove relevance or perish--that's the new motto.

And so, creative CISOs are getting out of their offices and seizing every opportunity to position security as a business enhancer. Securing virtualized environments is one of those areas where security leaders are grabbing big wins in the perceived value of IT security to the organization's business. Here's the language they're using with business owners:

- **Stealing the business is now easy.** Portability of virtual hard drives means the intelligence and processing of an entire business could be stolen, not just slowed down or hindered. This "lose-my-business" risk rather than the old "lose-my-bonus" risk should drive executives to allocate some operating budget for security.
- **Business applications are more vulnerable to security threats.** We don't understand the new class of vulnerabilities associated with this new thing called the hypervisor. The chance that critical applications running in a virtualized environment could be crippled by unknown vulnerabilities is now much higher. Low-cost architecture, zoning and security policy refreshment can go a long way to mitigating the unknown.
- **Invest with confidence.** If virtualization is here to stay, business owners are salivating at a faster path to introducing new technical functionality that can expand business capabilities. Virtualization can be a risky investment. Security's role is to validate when additional investment using virtualization is being made wisely and securely.

The security implications of this new world are becoming clear to security teams. In a year when IT security leaders have to prove relevance in the minds of both business executives and IT, securing the virtualized world should be a top priority.

*Jack Phillips is co-founder and CEO at IANS, an independent research firm based in Boston. Send comments on this column to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

Information Security Magazine is a part of the [TechTarget](#) portfolio of enterprise IT-focused media.  
Copyright 2000 - 2009, TechTarget. All Rights Reserved.