https://doi.org/10.48009/1_iis_2009_513-519

VIRTUALIZATION AND SECURITY: A PERSPECTIVE

James A. Sena, California Polytechnic State University,jsena@calpoly.edu

ABSTRACT

Extensive attention has been given to the topic of virtualization. Every aspect of IT has been affected by some form of virtualization. It also has another side – that of the virtual enterprise. We constructed and discussed a map of the facets of virtualization. We created a second diagram of the IT infrastructure containing three parts: computer hardware and software; the mobile worker activities: and internal operations of the organization. This formed the basis for discussion and related security problems. We described and commented about the IT infrastructure and the virtual organization. We noted that security has not holistically been addressed across the infrastructure and addressed some of the shortcomings and suggested ways to address these issues?

Keywords: Virtualization, Virtual Office, Mobile Computing, Server, Application and Network virtualization, Security

INTRODUCTION

In our examination of the current Information Technology [IT] environment we note that there is extensive attention being given to the topic of virtualization. Every aspect of IT is affected by some form of virtualization. It also has another side – that of the Virtual Enterprise or Organization. The use of "Organization" is probably more appropriate because there is a tendency to equate virtualization with the Enterprise in the context of IT only.

In thinking this through we constructed a map of some of the facets of virtualization. These are presented in Figure 1. On the left we have placed the physical organization -- consisting of two parts the IT infrastructure and the physical infrastructure. On the right we placed the Virtual Organization. Almost as much as the discussions about IT virtualization we have seen references to the virtual or mobile worker, the virtual workplace, and less so the virtual supply chain. Most organizations are typified by their mobile worker deployment – 365x24x7 -- anywhere, anyplace, anytime. To stay competitive organizations are foremost focusing on their core competencies while outsourcing or contracting their non-core processes. From both the physical and virtual sides the organization structure; the way that business processes are managed; and, the value/supply chains are changing and adapting to these business practices.

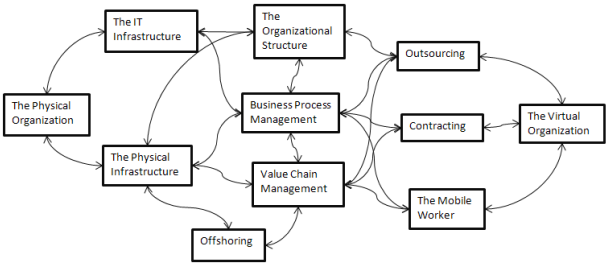

Figure 1. Some Facets of Virtualization

Our next step in trying to think this happening through was to create a second diagram of the IT infrastructure (see Figure 2). We organized the diagram into three parts. The typical virtualization part is the computer hardware and software. The organization part is the mobile worker and outsourcing (as well as contracting) activities. The intersection of these two parts deals with the internal operations of the organization; its relations with suppliers and the supply chain; and, its communication and management of customer relations.

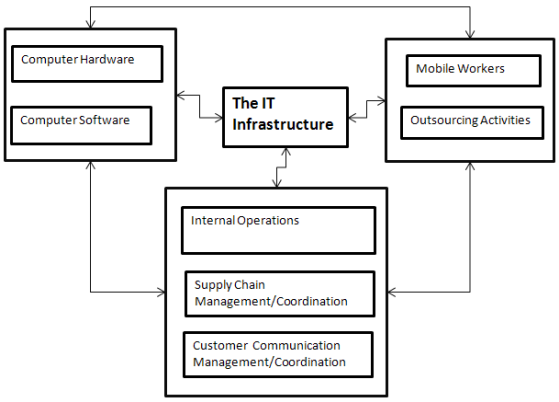

Figure 2. IT Infrastructure

In the rest of this paper we have selected excerpts from whitepapers and professional works to describe and comment about the IT infrastructure and the Virtual Organization. We note that security has not holistically been addressed across the infrastructure

We conclude with some implications and suggestions.

THE VIRTUAL ORGANIZATION

The term, "virtual organization," has no consistent meaning [1]. It has been applied to movie production, in which personnel come together for the duration of a project; just-in-time manufacturing operations, in which subcontractors simultaneously act as a manufacturing firm's supplier and warehouse; "adhocracies", in which specialized task forces and work groups arise and disband on demand; and informal regional consortia, in which material and personnel flow through the companies in a geographic area. Although these examples do not provide a tight definition, they suggest some of the features that underlie the concept a virtual organization. First, production processes transcend the boundaries of a single firm, and as a result, are not controlled by a single organizational hierarchy. Second, and perhaps as a result, production processes are flexible, with different parties involved at different times. Third, the parties involved in the production of a single product are often geographically dispersed. And finally, given geographic dispersion, coordination is heavily dependent on telecommunications and data networks rather than physical travel, at least for the people involved.

Much of the literature on virtual organizations rests on two assumptions The first is that firms adopt virtual forms in order to gain benefits of acquiring goods and services from specialized producers, who are able to make these inputs more efficiently [2]. The second assumption is that modern computer and telecommunications networks sufficiently reduce the costs of coordination, allowing firms to achieve these production benefits without incurring the higher transaction costs traditionally associated with buying from an external supplier [3].

For most firms, being virtual is a matter of degree. The production of any complex good or service requires combining various raw materials and modifying them in many stages, with each step adding value as the product wends its way towards the final consumer [4]. At one extreme, a firm is virtual to the extent that each of these steps is performed outside the core firm's boundaries, with the firm acting as coordinator. Some publishing operations approach this extreme, with no writing, editing, printing, and distribution done within the firm itself. But this non-value-adding structure will rarely arise in competitive business environments.

In the case of physical production processes this involves deciding whether to make or to buy each component of the product. For services, it is often the choice between using in-house staff or external consultants, freelancers, or specialty firms. Most organizations are situated between these extremes. Rather than expect to find virtual organizations, "virtualization" of organizations is better viewed as a continuum. Firms become more virtual when a larger proportion of important production processes occur outside of traditional organizational boundaries.

Security Issues: The Changing Boundaries (Globality)

As organizations stretch their wings and adjust to operate in a world without boundaries management must take steps to eliminate the distance between data centers and remote and mobile workforces. Access to business-critical applications and data, while maintaining a secure environment, is critical. While most companies talk about an economy that ignores national boundaries. “outsourcing,” Gartner [5]) suggests a focus on what they call “globality” and “insourcing.” Globalization is about the process of going global—and most companies are already there.

Globality, on the other hand, is more like a condition, where companies deal with a worldwide, interconnected economy that ignores national boundaries. Globality is forcing organizations to deal with employees on the move, remote offices in the far reaches of the world and data centers that house a company’s crown jewels. They need to pave the way for innovative business practices, closing the gaps, and enabling dispersed teams, distributed decision making and dynamic collaboration. The result is an organizational infrastructure that operates on an entirely new playing field, with more opportunity and responsibility. As IT takes the lead in adjusting technology the firm needs to address globality. They find themselves evolving from a necessary cost center to a valued business enabler to an indispensable business driver [6].

With IT departments in today's economy being asked to do more with less, virtualization's attractiveness becomes increasingly irresistible. But as some departments rush headlong toward the technology in an effort the stretch scarce dollars, the temptation arises to skimp on security [6]. Many thrifty managers believe that the same technologies currently used to protect conventional physical servers can simply be extended to virtualized

environments. This could lead to calamitous assumptions. The unwary could be trapped by threats in several areas, including software, administration, mobility, the operating system and network visibility.

According to Roberts [7] security experts are painfully aware that clamping down on insider threats and data leaks is an order of magnitude more difficult than stopping malware. And while recognition of the data-security problem is spreading fast within enterprises, very few have taken steps to lock down their sensitive data and intellectual property. Based on data accumulated on risk assessments of customer networks, approximately 2 percent of all sensitive or confidential files are exposed to theft by unauthorized personnel, and around one of every 400 e-mails that leave a company exposes sensitive data — either sent to an unauthorized recipient or sent to an authorized recipient in an insecure form that can be sniffed or otherwise stolen. Companies usually overlook that exposed data because their security posture is still focused on network perimeters, not on what might be going on behind the firewall or even over secure connections with business partners and suppliers. The perimeter around data is shrinking. Between joint ventures and collaborative [business to business] stuff and remote users, the perimeter has become highly porous.

There are some common-sense defensive steps, such as using firewall controls to limit user access and running a full array of security protocols and checks on each virtual server. There can be holes in the virtualization software --kernel attacks, someone attacking the host module or making a mistake against the host server. Beyond technology-driven measures, it's helpful for enterprises to keep details about virtual environments close to their vests in order to deter unwanted attention.

Virtualization: The Mobile Worker

As information technology has become more pervasive, the structure of the traditional work environment is continuously changing. A number of alternatives have emerged where work is performed at remote locations. Existing work practices and managerial strategies are often not appropriate in those environments. In particular, traditional office communication with coworkers and management, usually dependent on physical proximity, has been disrupted. One study [8]. found that telecommuters reported higher satisfaction with office communication. There also are indications that task predictability, IT support, and electronic coordination had similar influences.

It turns out most U.S. workers (70 percent) still commute to work every day, while just 2 percent telecommute full-time, according to the 2006 National Technology Readiness survey. The U.S. share of telecommuters would grow to 25 percent if it were practiced by everyone who had the option to telecommute and had the kind of job amenable to telecommuting, and this would save $3.9 billion per year in fuel costs. At the crux of the issue are trust and productivity. Managers have to trust the telecommuter's work ethic and must have a measurable approach to productivity. Employees have to recognize [the manager's needs], and demonstrate their productivity even more so when remote and stay engaged with the rest of the workforce.

Laptops have become so inexpensive that they're standard equipment at many enterprises. BlackBerrys are endemic among many levels of management and knowledge workers (even President Obama had to have his BlackBerry). Cell phones and PDAs are merging into smart phones that allow mobile e-mail, Internet and even corporate network access, as well as the ability in some models to work on spreadsheets. Copying company data onto USB thumb drives and other removable media has never been easier. Critical enterprise information is leaking onto mobile devices whose risk of loss or theft is much higher than it is for PCs at the office.

Concurrently, greater mandates for corporate accountability and regulatory compliance—with the Sarbanes-Oxley Act, HIPAA and the European Union Data Protection Directive, for example—are driving organizations to improve the tracking and management of corporate data. Toward this end, most organizations are embracing IT centralization and consolidation in attempt to enhance corporate control while curbing IT and operating costs. As a result, applications are tasked to take up the business slack outside of corporate headquarters. More and more applications—in kind, in number and in size—are chartered with carrying out key business functions and transactions.

According to a Citrix whitepaper [9] the workforce is now categorically distributed and mobile —working from remote offices, the road, home, wherever. And outsourcing is further extending organizational reach. With this movement comes an associated vulnerability. Security becomes ever more important, and elusive. It's not easy to control and protect corporate assets and resources, like business-critical data, when they exist outside of company constraints.

If customer financial information is compromised, for example, a single security breach can cost millions of dollars not to mention priceless consumer confidence. Without ironclad business continuity safeguards in place to deal with acts of war, nature or otherwise, one failed system can bring an entire organization to its knees.

The best way to secure company data is not to store it on client devices in the first place [10]. If data resides on servers and within the data center, with access permitted only over the network, there is no local copy to lose if a laptop or PDA is stolen or lost. This strategy also protects PCs in the office; after all, they can be stolen as well. While it can be more convenient for an employee to work from a local copy of data—on a laptop transported home or on a thumb drive—the high availability of broadband access and the maturity of remote-access technologies, such as laptops and smart phones, is rarely much less convenient.

VIRTUALIZATION" THE HARDWARE – SOFTWARE PERSPECTIVE

From a hardware perspective there are three basic categories of virtualization – storage, network, and server. Storage virtualization melds physical storage from multiple network storage devices so that they appear to be a single storage device. Network virtualization combines computing resources in a network by splitting the available bandwidth into independent channels that can be assigned to a particular server or device in real-time. Server virtualization hides the physical nature of server resources, including the number and identity of individual servers, processors and operating systems, from the software running on them. This last category is the most common application of the technology today, and it is considered the primary driver of the market [11]

Virtualization [12] refers to technologies designed to provide a layer of abstraction between computer hardware systems and the software running on them. By providing a logical view of computing resources, rather than a physical view, virtualization solutions make it possible to do a couple of very useful things: They essentially to trick the operating systems into thinking that a group of servers is a single pool of computing resources. And they allow the running of multiple operating systems simultaneously on a single machine. Virtualization has its roots in partitioning, which divides a single physical server into multiple logical servers. Once the physical server is divided, each logical server can run an operating system and applications independently. In the 1990s, virtualization was used primarily to re-create end-user environments on a single piece of mainframe hardware.

Hundreds, even thousands, of applications serve as the lifeblood of each of today's distributed global enterprises—at use in more places and in more ways than ever before. To deal with the growing complexity and cost of application deployment, maintenance and performance, organizations are looking for solutions to streamline, secure and manage delivery of their most business critical applications. In the process, these organizations are finding that traditional application deployment is just not up to the challenge. Instead, new approaches to application delivery are needed to address the changing world of business, where an increasingly dynamic workforce—whether employees, outsourced, or partners—must have access to applications at anytime and anywhere around the world. Fast emerging as the solution of choice is a virtualized application delivery model, which delivers only an application's "interactive" components to the end user while the application itself remains in the datacenter. This highly flexible approach enables organizations to quickly and cost-effectively deliver all of their business critical applications with security and control dramatically superior to traditional application deployment. Organizations have seen vast improvements in many key business arenas including branch office productivity, mergers and acquisitions, outsourcing, carbon footprint rollbacks and regulatory compliance.

Virtualization is changing the way resources are deployed and managed, simplifying and speeding IT response to a changing business environment [13]. It reduces IT management requirements and expenses by running multiple applications and operating systems independently on a single server. And it prioritizes business needs and maximizes server resources by quickly moving workloads from one virtual workspace to another. It allows the running of multiple applications and operating systems independently on a single server. Additionally, administrators can quickly move workloads from one virtual workspace to another - prioritizing business needs while maximizing server resources.

Server consolidation has become the cornerstone for enterprise money-saving initiatives. Industry analysts report that between 60 percent and 80 percent of IT departments are pursuing server consolidation projects. By reducing the numbers and types of servers that support their business applications,

companies are looking at significant cost savings. Less power consumption, both from the servers themselves and the facilities' cooling systems, and fuller use of existing, underutilized computing resources translate into a longer life for the data center and a fatter bottom line. And a smaller server footprint is simpler to manage.

Most companies begin their exploration of virtualization through application testing and development. Virtualization evolved from running extra operating systems into mainstream tools for software developers. Rarely are applications created today for a single operating system; virtualization allows developers working on a single workstation to write code that runs in many different environments, and perhaps more importantly, to test that code. After these application developments are realized, and the server farm is turned into a seamless pool of computing resources, storage and network consolidation are usually addressed. Other virtualization-enabled features and capabilities worth considering are: high availability, disaster recovery and workload balancing.

In the days of physical servers, it was in some ways much easier to manage the relationship between an application, the servers upon which the application ran, and the physical connections to those servers. But with the use of server virtualization, when a single physical server runs multiple applications, and when at any given time an application could be running on any one of a number of servers, Data center network managers now need a way to "reconnect" physical resources and virtual workloads in order to understand how they are being utilized and how to manage them [14].

Application virtualization relies on "isolation" technologies, or what is sometimes referred to as "sandboxing," to circumvent deployment (i.e., children playing in their own sub-sandboxes with their own toys won't fight over toys with other children in their own sub-sandboxes in the larger sandbox). Applied, virtualization abstracts applications from the host operating system to run on any device as well as share resources with conflicting applications. The application guts are isolated on the host, while the code necessary for interaction is dynamically coupled and reassembled on the fl y for the best on-demand user experience.

Virtualizing applications requires two kinds of virtualization technology to be at work in order to accommodate all user work scenarios: server-side and client-side (also referred to as "application streaming") virtualization. With both technologies integrated in a single solution, virtualized applications automatically select the best application delivery method based on user profile, application type and physical location.

Server-side virtualization is what typically comes to mind when referring to application virtualization — whereas the application is stored at the datacenter and abstracted from the user device. Because a small auto-updating virtualization client runs on the user's computing device, and not the client application, users can use the application from nearly any device (home PC, PDA, kiosk) that can connect to the host server in the datacenter. The only requirement is a network connection.

Client-side virtualization, on the other hand, enables the same level of access and control without the need for a network connection. The application is temporarily isolated on the user device while off-line, and then automatically synchronized with the datacenter once a network connection has been re-established. In this case, the user device behaves like the server.

In addition to its impact on data centers, virtualization is emerging as a viable technology for smartphones and virtual private networks, as well as being used to re-conceive agile and cloud computing. While it might be easy to think of virtualization as adding a software layer that requires additional controls to maintain security, proponents of virtualization argue that it serves the opposite purpose, and instead represents a core enhancement to security. Proponents of virtualization say that, in addition to facilitating new ways of enforcing security, virtualization technologies are leading to new ways of distributing software. The big problem with virtualization right now is performance guarantees [15].

IMPLICATIONS OF VIRTUALITY

IT departments everywhere are being asked to do more with less, and the name of the game today is resource utilization. Virtualization technologies offer a direct and readily quantifiable means of achieving that mandate by collecting disparate computing resources into shareable pools [12]. Fewer machines means less daily power consumption, both from the servers themselves and the cooling systems that companies must operate and maintain to keep them from overheating. This lessen the scope of future hardware expenditures.

Many companies have issued laptops as the standard PC, a strategy that undercuts security. Perhaps only employees who need to work while traveling should be issued laptops; examples include senior executives, salespeople, auditors, field technicians, some marketing staff and telecommuters. The rest might instead use PCs or computers at home or at satellite offices. Until software vendors have appropriate tools to cover the risks associated with mobile devices the organization will need to set policies banning or at least discouraging their use.

The advantages of virtual application delivery reverberate throughout the enterprise, streamlining many organizational imperatives. Here are some of the key areas where virtualized applications can make a dramatic difference: Planned or unplanned, system outages can cripple productivity, especially when key business applications aren't readily available. Virtual and network-based delivery enables workers to access their applications from any Web-enabled device as though it's business as usual. With multi-site deployments, users are transparently redirected to an available site, if necessary. All the while, valuable business information remains protected. And disaster recovery won't entail time-consuming and costly desktop rebuilds.

Complying with government or industry regulations is close to impossible without centralized control over corporate data. Audits take up a lot of time and money unless key data is close at hand. Virtualized applications keep important business information at the datacenter where it is quickly, securely and dynamically synchronized with online and off-line access. Change management for Sarbanes-Oxley Act compliance, for example, is greatly simplified as IT doesn't need to test upgrades and patches for silo conflicts to ensure applications stay in compliance.

Virtualized applications readily provide users at remote offices secure application access without having to deploy IT support and resources to those distant locations. With centralized management, IT can troubleshoot problems on the datacenter server—shadowing user sessions, for example, to track movement and errors. This saves considerable time and money while ensuring remote office applications work at peak performance.

Another consideration rests with business continuity. This is not just a good business practice - it can mean success or failure if data and applications on a production server are lost [16]. Disaster recovery planning ensures organizations have the capability to continue essential functions across a wide range of situations that could disrupt normal operations. High availability is the cornerstone for most business continuity plans and is one of the most compelling reasons for evaluating and deploying data protection solutions. However, traditional data protection strategies focus on just the data and not the application

Virtualization can go a long way toward reducing the physical requirements of the data center, but it can also compound the level of management complexity of those servers. There is a need for solutions that provide cross-platform systems management for both the virtual and physical machines. If the organization has not done so the ability to migrate their legacy applications and existing operating systems, without modification, onto virtual partitions needs to be addressed. This migration should make it simpler to enhance the performance of those applications, but solutions need to be place that supports the integration of virtualization with legacy management tools.

The sheer size and complexity of today's enterprises makes it nearly impossible to keep up with the rate of change in IT security, requiring a top-down strategy that prioritizes risk and accepts the limitations of available technologies [17]. Only through the adoption of high-level policies and controls aimed at fostering flexible security practices across the organization and via more aggressive sharing of information about threats with other , their partners, the supply chain, and the customer interface can companies effectively improve their protection and continue to do business as usual.

REFERENCES

1. Kraut, Robert, Steinfeld, Charles, Chan, Alice, Butler, Brian, and Hoag, Anne (2006) Coordination and Virtualization: The Role of Electronic Networks and Personal Relationships. Journal of Computer-Mediated Communication, Volume 3, Issue 4, Published Online: 23 Jun 2006
2. Davidow, W., Malone, M. (1992). The virtual corporation New York : Harper.
3. Malone, T., Yates, J., Benjamin, R. (1987). Electronic markets and electronic hierarchies: Effects of information technology on market structure and corporate strategies. Communications of the ACM, 30, 6, 484–497.
4. Porter, M. E. (1980). Competitive strategy: Techniques for analyzing industries and competitors New York : The Free Press.

5. Gartner Solutions (2007) Magic Quadrant for WAN Optimization Controllers, December 14, 2007, ID Number: G00153256.
6. CACM Reports (2009) The Changing Human Relationship with Computers: Impact of User Evoilution from Desktop Systems to Mobil Interfaces. 25 March 2009
7. Roberts, Paul (2009) Secure your enterprise data. InfoWorld IT Strategy Guides at http://www.infoworld.com/ad/sponsored_resources.html.
8. Fritz, Mary, Narasimhan, Sridhar, and Rhee, Hyeun-Suk (1998) Managing virtual workplaces and teleworking with information technology. Journal of Management Information Systems Volume 14 , Issue 4 (March 1998) Pages: 7 - 28
9. Citrix (2008) The End of Application Deployment: Virtualized Applications Streamline, Secure and Manage Your Business. www.citrix.com. 2008
10. Gruman, Galen (2007) ABC: An Introduction to Mobile Security – CIO, March 08, 2007 From: http://www.cio.com
11. Soror, A.A. Aboulnaga, A. Salem, K (2007) Database Virtualization: A New Frontier for Database Tuning and Physical Design. Data Engineering Workshop, 2007 IEEE 23rd International Conference (April, 2007)
12. Waters, John K (2007) ABC: An Introduction to Virtualization-CIO, March 15, 2007 From: http://www.cio.com
13. Dell (2009) Virtualize at the Speed of Your Business. Dell Virtualization.htm
14. Kroeker, Kirk. (2009) The Evolution of Virtualization. Communications of the ACM, Volume 52; Issue 18, 31 March 2009
15. Business Value Whitepaper (2007) Virtualization Technologies and their Impact on Disaster
16. Hines, Matt (2009) Enterprise security remains a balancing act. InfoWorld IT Strategy Guides at http://www.infoworld.com/ad/sponsored_resources.html
.