

Toward the Strategic Security Imperative:

**Integrating Automated Patch & Vulnerability Management into an
Enterprise-wide Environment**

CRA Reports

*This report was prepared by
CRA Reports, an independent
reporting agency based in
Washington, DC.*

**Copyright © 2005
All rights reserved**

Toward the Strategic Security Imperative:
Integrating Automated Patch & Vulnerability Management into an
Enterprise-wide Environment

By
Lane F. Cooper
CRA Reports

This brief White Paper explores the trends that are creating requirements for a strategic -- rather than a tactical -- approach to information security, patch and vulnerability management among public and private sector organizations. It demonstrates how an integrated, automated and enterprise-wide strategy that uses best-of-breed security solutions can be most effectively integrated into the operations of organizations large and small.

Despite the headlines, the conferences and the stated objectives of many large public and private organizations, many executives still wrestle with how to effectively deploy security measures that protect critical information assets underpinning their mission critical operations. It is the position of this White Paper that the challenges many organizations face in markedly reducing the risk posture of their organizations stem from a tactical understanding of risk and vulnerability assessment, perimeter security, threat remediation including anti-spyware, patch management and other critical security activities. Today, many organizations still treat each of these activities in a distinct and discrete manner, making it difficult to get a big picture understanding of their risk posture, inhibiting their ability to respond appropriately and cost-effectively to threats.

...A Growing IT Target

According to analysts at IDC, worldwide spending on information technology will grow at 6 percent a year through 2008 to reach 1.2 trillion dollars, up from 965 Billion in 2004. That increase in spending is an explicit recognition of the role IT plays in helping organizations to achieve their strategic business objectives.

However, it also represents a growing target of opportunity for those who wish to exploit our growing dependence on technology. This helps explain why in the United States alone the market for information security will grow at 19 percent a year through 2008, according to recent data from the Freedonia Group. That is more than three times the rate of the global IT spend. According to the Freedonia analysts, much of this growth will be driven by efforts to integrate security on an enterprise-wide basis.

...Security Still Afterthought

It would seem that people are voting with their wallets, and acknowledging that security is indeed a strategic issue. But is there truly a broad strategic recognition of security's strategic imperative? Consider the following:

- In the summer of 2004, a survey by the Conference Board revealed that almost 40 percent of respondents consider security an overhead activity that must be minimized.

- The situation appears no better in the public sector. Agencies in the federal government continue to struggle with meeting the requirements of Federal Information Security Management Act (FISMA). In early 2005, the Government Accounting Office (GAO), the investigative arm of Congress, concluded that poor information sharing and management was responsible for exposing homeland security to unacceptable levels of unnecessary risk.

The problem illustrated by the above points is not one of effort or discipline. Millions of dollars are invested on security technology and hundreds of thousands of man hours are brought to bear on protecting critical information assets by IT and security personnel.

The problem, rather, is one of perspective. In both cases, security measures appear to be treated as stand-alone activities that are divorced from the technologies, business processes and information assets they are meant to protect. Security, in short, is treated by many organizations as an afterthought.

"One of the greatest threats to enterprises today is that many – too many – organizations still consider security the lock they put on the door after the house gets built." -- Sean Moshir, CEO, PatchLink Corporation

The result is a tactical approach to security that is:

- **Fragmented**, because it is implemented in a stove-piped fashion in different departments;
- **Manual or minimally automated**, because point solutions cannot effectively interact with each other;
- **Disjointed**, or at least not well integrated with the applications they are meant to protect; and finally
- **Blind**, in the sense that is difficult to get a clear, complete and accurate picture of an organization's security posture.

It is also costly. According to recent research from Yankee Group, it can cost as much as \$1 million to manually deploy a single patch in a 1,000-node network environment. The firm has documented an instance in which an organization spent \$2 million to rush a patch in a telecommunications network that had 500,000 nodes.

"What contributes to these costs? It is the manual labor, the fixing of problems, the downtime for businesses while the patches are being deployed." -- Phebe Waterfield, Senior Analyst, Security Practice, Yankee Group

Waterfield confirms that many organizations remain highly reactive in their approach to patch management, and therefore have not developed automated and integrated strategies for making sure that the most current measures are in place within the enterprise to deal with known threats to their IT assets.

This contributes to a reactive and expensive approach to security that does not make progress toward the goal of reducing an organization's risk posture.

...A Changing Threat Picture

Hackers, authors of viruses and other sources of threats have become a major cost of doing business in the digital economy. Their handiwork is now covered by the mainstream media as well as the business and technology press. Their destructive impact on the economy is measured in the billions – if not trillions – of dollars.

And while organizations may be struggling with how to protect their information assets in an integrated and strategic manner, hackers and virus authors do not suffer from this angst. We are seeing the rise of hybrid threats in which viruses are used as launching points for initiatives that are designed to gather sensitive corporate data and/or execute identity theft.

For instance, spam is being used for phishing (an online con in which a "fake" site is set up to attract victims and solicit sensitive information from end-users), at which point spyware/malware or viruses are planted on consumer computers, while simultaneously gathering information that makes it easier to hack into the networks of the organizations they are spoofing.

As a result, we have seen attacks on enterprise networks become much more sophisticated and focused.

"This is why a tactical approach to security simply doesn't cut it anymore...especially when the threat picture to digital assets in all enterprise environments has become so acute. Where once the hacker community may have been seen as kids playing games, today we see malicious activity that is profit driven in some cases, and guided by fanaticism in others." -- Sean Moshir, CEO PatchLink Corporation

...A Strategic Response

A growing number of large organizations are recognizing the imperative for the IT community in general -- and the information security community in particular -- to move away from a tactical perspective of their role, and become a more strategic element in their organizations.

"In 2004, our technical operations organization adopted ITIL [the IT Infrastructure Library] to develop a long term strategy for providing IT services. We embraced an IT service management model that is a top-down, business-driven approach to the management of IT that specifically addresses the strategic business value generated by the IT organization and the need to deliver a high quality IT service. We immediately recognized that security management touches a number of the high level processes including infrastructure and application management, service delivery and service support. So we have integrated our security operations into this service management paradigm." --Tim Mathias, Chief Security Officer (CSO), Thomson Financial

According to PatchLink's Moshir, an effective strategic response to these threats must consist of four basic elements. It must be:

- **Enterprise-wide.** Security efforts must be fully integrated throughout the entire enterprise -- and in some cases the extended enterprise -- so that threats can be addressed in a unified manner. In its most simple sense, once a threat has been dealt with, the entire organization should be prepared to address it should it manifest itself again anywhere else within the domain.
- **Fully Automated and Integrated.** Given the rapid pace of new threats and vulnerabilities, there is no room for a manual response. Security systems must be able to behave in an integrated manner. This means that perimeter security must be linked to intrusion detection systems, and that vulnerability assessment activities must be linked to remediation, and so on and so forth.
- **Dynamic.** Information security should be seen as a business process -- or better yet: as an integral part of all business processes. As such it is not an event that can be installed and forgotten. Technology, people and evolving best processes must be constantly developed, tested, deployed and re-evaluated.
- **Visible, Measurable and Standardized.** There should be nothing mysterious about the security strategy. It should be easy for non-technical executives to understand. The data gathered by sensors and reporting tools should be presented in ways that are meaningful to the users who must make decisions based on that information. And the data must be standardized so that information from one security system makes sense to the rest of the organization.

"From a management standpoint, there must clarity and transparency within and between all security systems. After all you cannot effectively manage what you cannot see." -- Sean Moshir, CEO, PatchLink Corporation

###

About The Sponsor:

PatchLink™ Corporation (www.patchlink.com) is the established leader for enterprise-wide, security patch and vulnerability management including end-point and anti-spyware solutions. Recognized by Inc. 500 as one of the fastest-growing companies in the United States, PatchLink's market-leading PATCHLINK UPDATE™ software is currently integrated and interoperable with several industry-leading, end-point security management platforms for real-time remediation.

Organizations using PatchLink software, solutions and services show a 95 percent-plus renewal rate and better than 97 percent of customers indicate they are "satisfied or highly satisfied" with overall product and service performance.

PATCHLINK UPDATE currently operates in every branch of the federal government, including the Army, EPA, USDA and NASA; global companies, such as Kraft Foods, Thomson Financial, Virgin Airways and Boeing; and major regional companies, including BlueCross BlueShield; and several academic institutions. With a strong reputation for providing unparalleled network and security management software products and services, PatchLink currently has one of the largest installed subscriber bases for patch and vulnerability management software.