

SMARTER SECURITY SPENDING: DRIVING ROI VIA PROACTIVE TESTING

Using Comprehensive IT Security Testing to Assess Vulnerabilities, Determine the Efficacy of Existing Defenses and Optimize Spending in a Budget-Constrained Economy

EXECUTIVE SUMMARY

This paper examines how comprehensive security testing allows organizations to better understand the return on investment of defensive solutions and where their most significant vulnerabilities exist to help target security spending in a challenging economic environment. It is meant to illustrate how actively testing the exploitability of vulnerabilities enables organizations to measure the ability of their defenses to deflect real-world threats. By actively testing these defenses in a conclusive manner, IT budgets can be more strategically aligned to determine how existing defenses can be improved, what additional systems may be needed, and how to directly address remaining risks.

UNCERTAIN ECONOMY IMPACTS SECURITY SPENDING

Over the last five years, the vast majority of organizations have incrementally increased their IT security budgets¹ to help defend their operations from the rising tide of malware infections and data theft incidents. They have also invested heavily in security systems needed to help them meet the requirements of the growing number of government and industry compliance regulations that mandate the adoption of stronger defensive controls.

During this same timeframe, executive management in many organizations has increasingly called for reductions² in overall IT budgets, with many companies seeking to streamline technology-related spending and maximize existing resources across the board. However, security plans have traditionally been insulated³ from more conservative planning based on the rapid proliferation of threats and regulations that have forced organizations to implement specific types of defensive mechanisms.

Now, with the recent uncertainty in the worldwide economy, driven by the rising price of vital commodities and the ongoing turmoil throughout global financial markets, many organizations worldwide have begun to more actively scrutinize their security budgets.⁴ In addition to trying to determine what types of investments will be most beneficial in achieving their security and compliance goals over the next several years, many are seeking to eliminate plans to acquire any technologies that will not deliver immediate return on investment or help address specific needs.

With no end to the current economic crisis in sight, and more organizations undergoing dramatic business transitions including mergers and acquisitions⁵ driven by the ongoing financial uncertainty, IT departments are being put under greater pressure than ever before to ensure that diverse, widespread assets are being adequately protected and that compliance requirements are being met, even as risks proliferate and their budgets and staffing levels are being reduced.⁶

As such, many organizations are looking for more substantive methods to directly assess the performance of both new and existing security defenses, and compliance controls, to better understand where their most critical vulnerabilities and risks reside and how they should target future spending.

LAYERED SECURITY FALLS SHORT

For close to a decade, most mature IT organizations have approached the process of defending their critical infrastructure and applications from security risks via the acquisition and adoption of layered defense technologies. By enlisting a broad range of perimeter and internal security point solutions including IPS/IDS, anti-virus, firewall, behavior monitoring and user authentication systems, among many other technologies, organizations have sought to address individual areas of risk and sets of attacks on an incremental basis.

Despite making sizeable investments in those products and enduring complex integration efforts to ensure that these security defensive mechanisms are as tightly aligned as possible, the continued evolution of cybercrime, malware threats and hacking techniques has left many organizations struggling to validate that their assets and electronic data are sufficiently protected from the full range of potential attacks.⁷

At the same time, the IT security industry continues to produce innovative new technologies that promise the ability to plug existing gaps in traditional defenses, such as in-the-cloud malware filtering systems, network access control (NAC) technologies and data leakage prevention (DLP) platforms. However, the lion's share of those tools remain largely untested in real-world scenarios and offer little

¹ Forrester Business Data Services survey, Forrester Research, Sept. 2008

² "Economic Gloom Puts Pressure on IT Budgets," IT Week, April 2008

³ "Security Spending Safe from IT Budget Cuts," Network World, Sept. 2008

⁴ "Economy Freezing IT Budgets, Survey Shows," Network World, Oct. 2008

⁵ "Tough Economy Prods Chip Merger Activity," Investors.com, Oct. 2008

⁶ "Wall Street's Collapse Dents IT Spending," PC World, Oct. 2008

⁷ "Cybercrime Toll Mounts," Network World, Sept. 2008

proof of their immediate return on investment, even though they carry sizeable price tags and demand sophisticated integration efforts to work smoothly in today's highly-customized environments.⁸

As a result, even the most deep-pocketed IT organizations have found themselves in the uncomfortable position of feeling vulnerable to emerging vulnerabilities and threats while facing the prospect of being forced to continue to invest in new technologies that may or may not address their specific security needs.

While few experts would seemingly endorse the suggestion that the layered approach to security is fundamentally flawed, it has become clear that organizations need a more effective manner of determining just how well their existing defenses are working, where those systems may be adjusted to improve their overall security posture, and how they can most intelligently distribute their budgets in the coming years to best protect their assets and garner maximum ROI from the technologies they choose to acquire.

DRIVING ROI VIA SECURITY TESTING

All of these aforementioned problems play directly to the strengths of comprehensive, independent security testing technologies that provide IT and compliance management professionals with increased visibility into their organization's overall security standing, and help staffers understand where gaps in their security point solutions still exist.

Rather than trying to complete complex, theoretical ROI calculations to determine the value of existing defenses or the potential impact of additional point technologies, organizations can use security testing to actively seek out any exploitable vulnerabilities and available paths to critical infrastructure or data to determine exactly where their most significant weaknesses reside.

By engaging in ongoing, proactive measurement of their security posture using commercial grade exploits that expose vulnerabilities but do not effect critical operations, organizations can immediately establish the ROI of the defensive technologies that they have already implemented and deduce which systems are not, or may not, provide optimal returns.

For IT budget decision makers, the use of comprehensive security testing also provides a tactical means of proving how well earlier investments and previously-implemented defensive mechanisms are working and highlights the ability of emerging threats to circumvent even the most intelligently aligned defenses and validate continued security spending.

Security industry experts, including analysts and consultants, have recognized the need for comprehensive testing capabilities delivered independently of defensive technologies to provide the most comprehensive and objective view into potential risks.⁹

As security point products continue to proliferate, even more pressure will likely be applied to those teams responsible for installing and maintaining the technologies to ensure that they are meeting goals and delivering sufficient ROI metrics, especially in the current challenging economic environment.

Enterprise customers that have already adopted comprehensive security systems agree that the most effective method for assessing their overall security posture, testing the efficacy and ROI of defense mechanisms, and proving the value of future point product investments is via adopting more consistent, proactive security testing to address all these challenges.

"The products we were evaluating cost hundreds of thousands of dollars. When making that level of investment, we have to be sure that the technology we implement can effectively mitigate problems," said Andre Gold, a former information security director at Continental Airlines and senior vice president of Security and Risk Management at financial services giant ING. "Testing is the only process that allows us to verify the impact of a potential vulnerability and prove that our security technologies are working and actually detecting and preventing attacks."

⁸ Data-leak security proves to be too hard to use," InfoWorld, March 2008

⁹ Case Study: Penetration-Testing Tool Use, Gartner, May 2008

CONCLUSION

Organizations that are determined to maximize their security budgets and defend future spending in an economically-constrained business environment should engage in comprehensive security testing to put a finer point on their efforts and make buying decisions more intelligently.

Those executives and managers responsible for creating and defending security spending should ask themselves a battery of questions including:

- How do I know that our existing defensive mechanisms are working?
- Can I derive additional value and protection from the systems we already have in place?
- What is the best way to determine what our most critical vulnerabilities are?
- How do we know whether or not new solutions will provide sufficient ROI?
- Is there a simple way to illustrate why we need additional resources to management?
- Can we eliminate unnecessary spending through proactive analysis?

By acquiring a commercial-grade security testing solution before making new investments in additional point solutions, organizations can ensure that they are getting the most out of the security systems they have already purchased, and prove that they are addressing their most critical risks by implementing the most appropriate defensive mechanisms and compliance controls.

The CORE IMPACT family of comprehensive security testing software solutions, offered by Core Security Technologies, represents the world's most mature, effective manner for organizations seeking a means to rapidly assess their critical vulnerabilities and determine the ROI of their defensive infrastructure.

For additional information on the CORE IMPACT family of comprehensive security testing products, please contact us at 617-399-6980 or via email at info@coresecurity.com. You can also visit our web site at www.coresecurity.com.