

Opening IT Security: A 3Com ROI Series Document

WHITE PAPER

Evolving Security

Once upon a time, IT managers and executives looked at the Security ROI equation and compared the results to the ROI of competing IT projects.

$$ROI = \left[\frac{(\text{Savings} + \text{Revenue Increase}) - \text{Investment}}{\text{Investment}} \right]$$

Should our IT dollars be spent on virus protection, firewalls, etc., or on new servers, database software, ecommerce systems, or any number of other competing projects? Which of the investments under consideration provided the greatest opportunity for return? And which represented the best financial investment? Thus, just a few years ago, you couldn't throw a virtual rock on the internet without hitting a paper, presentation, or sales tool attempting to "make the business case" for an investment in Security technology and products.

Today that question couldn't be more irrelevant. Every C-level executive worth half their salary fully appreciates the need to protect an organization's assets from the disgruntled employee with an axe to grind, the 17-year old hacker in his bedroom in Wisconsin looking to impress his buddies by launching the next Sasser virus, the 21st century Billy the Kid robbing banks not with a revolver but with a laptop and high speed connection, or the "angry young man" with a cause who would like nothing more than to splash an anti-war slogan on the home page of a defense manufacturer.

The sheer number and diversity of threats to critical organizational information and functions has forever altered the discussion from one of "benefits" of a Security investment, to the "best, most flexible and cost-effective means" of obtaining the protection no one disagrees is necessary and vital to run a modern organization.

In this new environment, the ROI equation hasn't changed, but the way in which CIOs use the results of the equation has. The ROI of a particular Security solution is now compared to the ROI of a competing Security solution, not to a different IT investment. Thus, the Security investment question has changed from "Do we invest in Security?" to "What is the best Security system investment?"

In this paper, we'll discuss how the newest, open architecture IT Security solution can both increase the cost savings to an organization (by improving Security and minimizing successful attacks), and also substantially decrease the cost of deploying flexible Security systems capable of protecting the organization-and its many departments or branches.

CONTENTS

Evolving Security.....	1
Less is More.....	2
Higher Learning in Security.....	2
More Boxes...More Everything.....	3
"We Have Met the Enemy, and He Is Us."	4
The End of the One-Trick Pony	6
Best of Breed and Tight Integration = Better Security	7
Spending and Defending Smarter	8

3Com Value Highlight
 Organization: Harrisburg Airport
 3Com Product: Security Switch 6200

Less is More

Harrisburg Airport in Pennsylvania is one of the first to avail itself of the new IT Security architecture available in today's market. The new \$220M airport facility was searching for a LAN solution that could provide IT Security not only to the airport facility (and its Internet-accessing passengers) as a whole, but also individually to its eight different airlines, six rental car agencies, and a railway operator. All 15 of these internal users required independent firewall and intrusion detection systems (IDS), protecting against outside threats as well as those internal to the airport facility. In addition, the airport required complete system redundancy, in effect doubling the total hardware requirement.

"The simplicity, security, and value of our new 3Com network exemplifies everything we want our new transportation complex to be...3Com stood out among other vendors in providing this solution."

—Mark Berkheimer,
 Manager of Information Technology,
 Harrisburg Airport

Conventional IT Security design practice calls for an individual hardware piece for a firewall, and yet another hardware box for its intrusion detection system (IDS). The cost ramifications of such a system design approach are underwhelming if one or two data flow points require protection, but cost differences are rapidly amplified when the requirement to protect upwards of 15 different entities redundantly is introduced. A more forward-looking approach borrows the time-tested IT cost reduction principle of server consolidation and applies it to IT

Security infrastructure design. Rather than run individual applications on one closed box, Harrisburg chose a solution based on running both firewall and IDS software on a single, open hardware platform; their chosen solution, the 3Com® Security Switch 6200, provided Harrisburg the flexibility to select from best-of-breed firewall and IDS solutions from Checkpoint and ISS, respectively. The bottom line: a 45% security systems costs savings over the only other bidder.

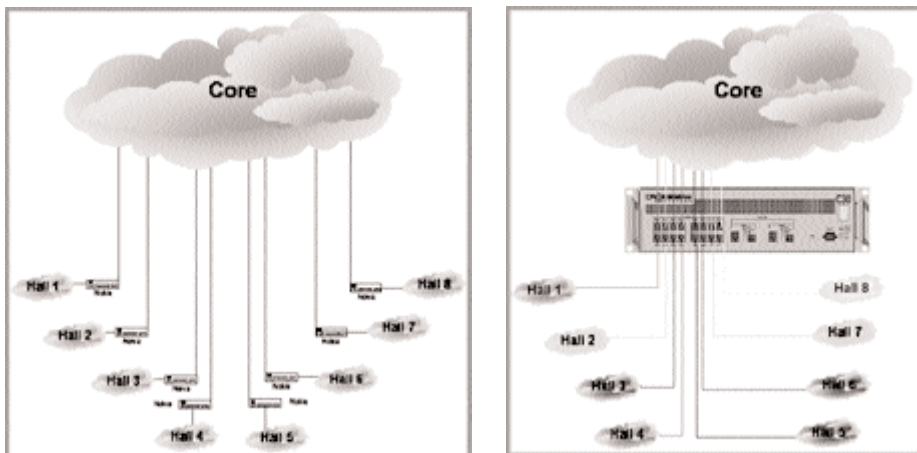
Further, as the Harrisburg hardware platform is capable of running three applications simultaneously, the airport can choose to add additional security applications at a later date without hardware modifications, choosing from Trend Micro, Aladdin, Secure Computing, Websense, or Snort.org as their Security requirements evolve. The architecture of the Switch 6200 and its associated cost savings and flexibility made Harrisburg's Security decision an easy one for Mark Berkheimer, Harrisburg's Manager of Information Technology: "The simplicity, security, and value of our new 3Com network exemplifies everything we want our new transportation complex to be...3Com stood out among other vendors in providing this solution."

Higher Learning in Security

The value of a hardware consolidation approach to Security was driven home for a major university in the US when an analysis was conducted comparing the non-recurring and recurring costs of different IT Security

systems needed to protect 93 university residence halls. One option comprised an appliance-based solution from a Fortune 100 communications company; the other was provided by 3Com with the previously-mentioned Security Switch 6200 as the primary element of the architecture.

FIGURE 1: Security Architecture Comparison: Conventional Appliance Topology vs. 3Com Open Approach



The first option (depicted on the left in the previous figure) required one appliance for each of the 93 residence halls, while the 3Com solution exploited the higher processing capacity and port density of the Switch 6200, providing the same performance with 12 total boxes.

Intuitively, a solution requiring 81 fewer hardware pieces should be less expensive to deploy and operate, and the analysis showed exactly that. Table 1 illustrates the fractional cost of the 3Com Security Switch 6200-based solution versus the appliance-based Fortune 100 approach from the perspective of acquisition, maintenance, and operational costs.

Thus, 81 fewer hardware platforms translate, over three years, into an overall solution that will cost less than half an appliance-based system to procure and maintain, while still providing an identical firewall solution. The early 20th century American humorist Kin Hubbard once said “The safe way to double your money is to fold it over once and put it in your pocket.” If he were alive today, he might have added that another way to do so is to invest in a 3Com Security Switch 6200.

TABLE 1: TCO Comparison of 3Com Security Switch 6200-based Firewall Solution Versus Appliance-Based for University Residence Halls

COST CATEGORY	PERCENTAGE COST SAVINGS WITH 3COM SOLUTION VS. APPLIANCE-BASED SOLUTION
Capital and Licensing Costs	43%
Maintenance Costs (Over 3 Years)	66%
Operational Costs ¹ (Over 3 Years)	18%
Total Solution Cost Projected Over 3 Years	46%

More Boxes....More Everything

Every IT manager knows that the financial pain inherent in doubling the number of required hardware platforms for a Security system—or any IT system for that matter—doesn't end with the initial cost of the additional hardware; it only begins. For example, according to a Meta Group estimate,

companies spend \$7 on management for every \$1 of infrastructure, while staffing costs—not hardware—make up about 60 percent of a typical IT budget. This reality is the fundamental driver behind the server consolidation strategy of many IT departments. Table 2, reproduced here from a Compuware white paper², illustrates the long-term value in minimizing the number of IT hardware entities in an organization.

TABLE 2³: IT Hardware Consolidation Value

COMPANY	PROJECT	RESULTS
American Management Association	Consolidation from 75 to 10 Servers	\$7.5 Million Savings in Staff and Operations
Wyndham International	Consolidation from 165 to 2 Servers	Lowered Hardware Cost by 40%
British Telecom	Consolidated from 100 to 6 Servers	Breakeven on Project in 18 Months
Corporate Express	Consolidated from 43 to 2 Servers	Operating Savings of \$10,000 Per Day
P&O Ferrymasters ⁴	Consolidate 45 Servers to 1	Project \$42,900 Annually in Maintenance Costs (Not including Staff)

1 The assumptions and other details of the operational cost and other analyses summarized here are beyond the scope of this paper and proprietary in nature. We encourage readers to contact your 3Com sales representative to learn more about the analysis.

2 “Essentials for Successful Server Consolidation.” Compuware Corporation. <http://www.compuware.com/dl/server.pdf>

3 Ibid.

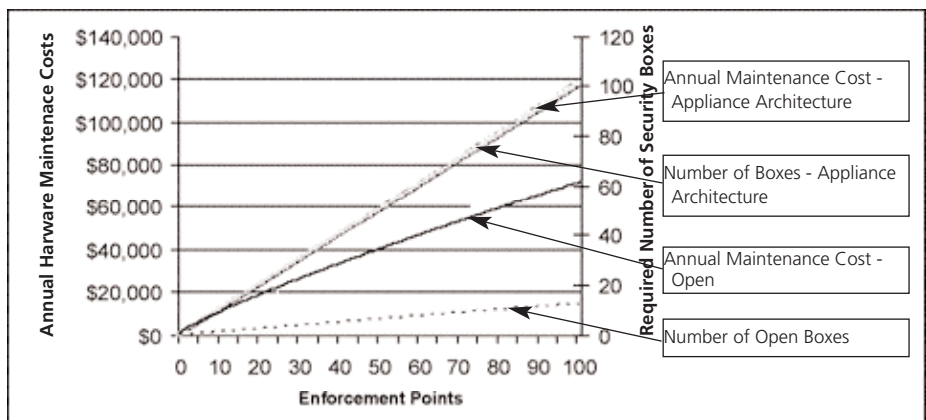
As homeowners and weekend boaters know all too well, it's not just the initial cost of the hardware, but the ongoing labor to keep it running.

Figure 2 below applies this basic hardware consolidation principle to Security hardware. As shown, as the number of enforcement points in an organization's system increases, the number of Security hardware pieces increases, as does the cost to maintain each individual hardware device. As shown, the box consolidation offered by the 3Com

Security Switch 6200 and the Security Switch 7200 Family of products reduces the cost to maintain the overall system, providing on-going Security system savings beyond the initial acquisition cost benefits.

The analysis accounts for the increased cost of maintenance of a more complex Security box, but unless the number of enforcement points is less than five or so, the on-going financial benefits of fewer, more flexible, more capable hardware devices is clear.

FIGURE 2: Hardware Maintenance Cost Comparison: Open Security System Vs. Conventional Appliance-Based Approach



“We Have Met the Enemy, and He Is Us.”⁵

To this point in the discussion, the Security solution has remained constant—and equally robust—across the platforms under discussion, and emphasis placed on solution cost comparisons. But can a more capable hardware platform also provide improved Security? Can flexibility translate into a measurably lower risk of Security breach incidents? Yes it can.

The 2003 CSI/FBI Computer Crime and Security Survey reported that the second most common form of network attack was insider abuse, reported by 80% of the survey's respondents (second only to virus incidents at 82%). If those statistics aren't frightening enough, the same report ranked disgruntled employees (77%) just behind independent hackers (82%) as “a likely” source of attacks⁶. Finally, the study noted that 45% of the participating companies

reported unauthorized access by insiders⁷. Often overlooked, securing organization IT assets not only from inside attacks, but also from the innocent but careless actions of employees spreading threats initiated outside the organization, is a real challenge for today's IT Security professionals. It's simply not sufficient for the IT department to build a moat around the organization's castle and relax.

So how can an innovative Security hardware architecture address the internal threat challenge? The answer lies in capacity and flexibility. Returning to both the Harrisburg Airport and university cases previously discussed, a key similarity between them was the need to secure multiple sites or entities within a single system—multiple “enforcement sites” or “security zoning” in the parlance of the IT Security professional. In those two cases, the multiple entities were different companies within a single airport facility, or multiple dormitories in the same University.

⁴ “P&O Throws Maintenance Costs Overboard”. <http://www.vnunet.com/news/1142017>

⁵ Pogo, comic strip written and drawn by Walt Kelly

⁶ Ibid as quoted in “Access Management and User Accountability for WLANs”, a Vernier Networks White Paper.

⁷ CSI/FBI Computer Crime and Security Survey, as quoted in “Information Systems Misuse - Threats & Countermeasures.” By Vijay Gawade. <http://www.itsecurity.com/papers/gawade1.htm>.

As discussed, one way of solving the problem—the way proposed by the Fortune 100 Company offering the first option in the University example—is to throw hardware at the problem; apply one box (or appliance) per independently secured entity. Without question, that approach will work, but as the old joke goes, although it is possible to clean the floor of Madison Square Garden with a toothbrush, there are better ways to go about it.

The same 3Com Security Switch 6200 capability that Harrisburg utilized and the University reviewed to address their multiple “customer” challenges can be employed by large organizations to secure the Human Resource department—and its wealth of highly confidential information—from the curious employee in the Marketing department, or the Department of Motor Vehicles records from the budding hacker in the State Comptroller’s Office.

Additionally, there may be an organizational need to provide different levels of access to different internal and external entities: it may make complete sense for the food supplier to the Pentagon’s Cafeteria to have access to its on-hand food inventory, but not to its intelligence databases, while the students at Central High School will require access to the teacher’s assignment web page, but obviously not the teacher’s grading records. All such requirements, and an endless list of others, drive the total number of enforcement

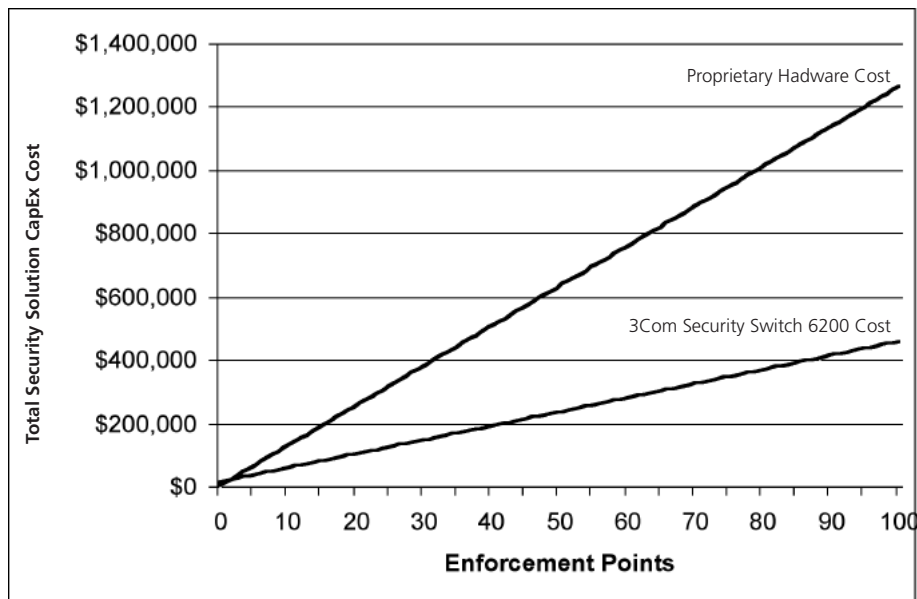
points in today’s security network, and the cost and complexity of the Security solution.

Figure 3 illustrates the difference between conventional Security architecture solutions and the open architecture of the Security Switch 6200 as the number of system enforcement points increases, while Figure 2, previously introduced, illustrates the ongoing cost ramifications of an increase in system enforcement points.

The exceptional throughput of the 3Com Security Switch 6200 and Security Switch 7200 Family products enables a single box to service multiple departments/enforcement points, and its flexible software architecture allows internal firewalling and the accompanying implementation of proper policy. Using these switches, IT Security professionals can apply a rich and granular set of rules to multiple departments independently, rules based not just on addresses but on protocols, ports, sockets, times etc. and combinations of these factors.

Most importantly, the goal of providing an internal Security web of many enforcement points to complement the externally-facing Security wall can be accomplished without the cost explosion inherent in competitive solutions; in a nutshell, the architecture of the Switch 6200 and Switch 7200 Family solves the internal security problem less expensively too.

FIGURE 3: Acquisition Cost Comparison - Proprietary Hardware Solution Vs. Open Architecture of 3Com Security Switch 6200⁸



8 For more details on the methodology and assumptions underlying this analysis, please contact your 3Com sales representative.

“When I learned that I could run both the firewall and the filtering on the same box, I said ‘This is great.’...and not only can I put different applications on the (Switch) 6200, but I can take them off down the road.”

—Steve Dantinne,
Supervisor of Technology,
Vineland School District

3Com Value Highlight

Organization: Vineland School District
3Com Product: Security Switch

The End of the One-Trick Pony

Medical trauma professionals are taught first to stop bleeding, then restore a patient's airway, and only then to address “minor” problems like compound fractures. However uncompassionate that may initially sound, such guidelines make complete sense: prioritize the problems, then address them in order. In today's Security environment, an organization's first priority—the bleeding, if you will—is clearly the prevention of malicious attacks from worms, viruses, hackers, and 20th century thieves. But as Security technologies, policies and architectures are rapidly evolving to effectively address these threats, other external content-related challenges are already emerging as the next problem.

A virus attack isn't the only threat to an organization's productivity in today's IT environment. Seemingly innocent employee activities can result in lost money, productivity, or even customers. Pop-up ads, spam⁹, and non-work-related Internet surfing eats network bandwidth and distracts employees¹⁰, while employees exchanging pornographic images may not only reduce overall productivity¹¹, but may also induce lawsuits¹². And one can only collectively wonder what currently unimagined headaches will steam into the network via the Internet and email in the coming years.

Steve Dantinne understands this benefit from a firsthand perspective. As Vineland School District's Supervisor of Technology, Steve is responsible for the network that supports over 5,000 computers, and also provides Internet service to other Vineland municipal agencies such as the Police Department and the Public Library among others (“We're like Santa Claus with the Internet” notes Steve jokingly.) Steve was delighted to learn that the 3Com Security Switch 6200 could provide not only the Checkpoint firewall protection he needed, but could also provide content filtering for the school district.

Especially attractive to Steve was the multiple software options available, enabling him to purchase only the content filtering capabilities he required. Steve looked at all the filtering options available on the Switch 6200, and chose the Secure Computing's product. The switch's capability meant Vineland no longer required a separate hardware device for content filtering, saving the school district between \$20,000 and \$40,000. Added Steve: “When I learned that I could run both the firewall and the filtering on the same box, I said ‘This is great.’...and not only can we put different applications on the (Switch) 6200, but I can take them off down the road.”¹³

As Vineland School District has learned, no Security hardware platform can predict the future, but it can be designed to maximize openness and flexibility, giving it the best chance to react to new and emerging content filtering challenges. Conventional Security appliances run a single Security application; there's a box for IDS, a different box for the firewall, and so on.

We've discussed the cost ramifications of such a limited architecture previously, but the lack of flexibility inherent in a fixed hardware solution can have significant consequences as the organization grows, or the content filtering challenges change. Open platforms like that of the 3Com Security Switch 6200 and Security Switch 7200 Family provide an architecture and throughput capacity that minimizes the probability of a stranded hardware investment.

With this ability to run three different content applications on the same hardware, the design of the switch has accounted for the dynamic nature of the external content threat. Today, the Security Switch 6200 and Security Switch 7200 Family products ship with binary files for seven Security applications¹⁴, and the number and types of content application options are likely to increase over time. Users of these open-architecture switches need only contact their preferred vendor for the license for the desired security or other content application.

9 Network Associates Reports that its internal research concluded that spam accounts for 50% of all email traffic (McAfee Security White Paper “Building Cost-Effective Security Solutions for Small-to-Medium Sized Businesses”. March 2004. <http://www.itpapers.com/abstract.aspx?scid=1100&docid=88956>)

10 IDC reports that 30% of web surfing is not work related. Arbitron reports that 77% of online listening to Internet Radio on weekdays takes place between 9am and 5pm. 44% of corporate employees actively use streaming media (NielsenNetRatings).

11 70% of pornography is downloaded between 9am and 5pm (SexTracker), while one-third of workers admitted to passing along pornography at some time and half of all workers said they'd been exposed to sexually explicit material by co-workers. (“Porn at Work Problem Persists”, Bob Sullivan, MSNBC, 9/6/04). <http://www.msnbc.msn.com/id/5899345>

12 The American Management Association reports that 27% of Fortune 500 Companies have battled sexual harassment claims stemming from employee Internet misuse.

13 Interview with Steve Dantinne, Vineland School District Supervisor of Technology. September 8, 2004.

14 Checkpoint, ISS, Trend Micro, Aladdin, Secure Computing, Websense, and Snort.org

Thus, one switch might be running a firewall and an IDS application, while the one sitting next to it applications from Websense and Secure Computing. Two years from now, those same two switches might be running a currently undeveloped application. As the CEO of a major Security software vendor recently noted: "About every 15 to 18 months, there's a new form of attack that makes the old technologies less effective."¹⁵ Flexibility and openness are popular marketing/sales buzzwords, but when talking about Security IT architecture, they translate into real value.

Best of Breed and Tight Integration = Better Security

Albert Einstein once said that everything should be made as simple as possible...but not simpler. Thus, long before the first computer hacker touched a keyboard, Professor Einstein would have appreciated IT Security author Bruce Schneier's maxim: "complexity is the enemy of security."¹⁶ As discussed, traditional Security solutions require separate hardware platforms for each Security application, so a typical enforcement point in an organization's Security system comprises a firewall, a switch, and a load balancer. Security experts refer somewhat pejoratively to this configuration as a "firewall sandwich". As more firewalls are required, more switches and load balancing are also needed. Add a separate server for content filtering, virus protection, etc., and Rube Goldberg would be proud.

We've discussed the cost ramifications of such Security architectures—and the unwieldy nature of their practical implementation, maintenance and operation are self-evident—but despite the operational shortcomings, can conventional Security architectures defend against today's threats?

The key to answering that question lies in the nature of sophisticated attacks. "Blended threats"¹⁷ like the Blaster and So.Big viruses require coordinated responses from multiple Security applications; that is, the IDS software and firewall must work in conjunction with

virus protection to effectively counter blended threats. An enforcement point pieced together with multiple applications from multiple vendors must be closely integrated and tested to assure the coordination required in today's threat environment, yet another task for the typically overworked IT department.

The new, open approach to Security platforms does that work for the IT department. The 3Com Security Switch 6200 and Security Switch 7200 Family not only offer multiple applications from best-of-breed vendors, but 3Com tests the applications on the platform, certifying the best combinations for individual Security needs. This system offers certified application clusters for network protection, web user protection, and email protection, for example, assuring that the applications not only co-exist, but work effectively together to counter blended threats. The open approach to IT Security offers not only best-of-breed virus, IDS, firewall, etc., but more importantly, integration of those best-of-breed products. No other system can offer both tested integration and best-of-breed quality simultaneously.

More importantly, an integrated, tested collection of Security software products comprising the best available software on the market will decrease the probability that an attack from a blended threat will penetrate the system. In the first half of 2003, organizations experienced an average of 38 attacks on their systems per week, with blended threats accounting for 60% of those.

Thus, security systems are being asked to defend against more than 20 blended threat attacks weekly¹⁸. Of course, few of these attacks are successful, but some are. The 2004 CSI/FBI Computer Crime and Security Survey reports that 18% of the respondents to the survey experienced more than six successful outside attacks in the previous 12 months, and an additional 52% reported at least one or more successful attacks¹⁹.

¹⁵ Business Week, June 21, 2004. Page 85.

¹⁶ "Essentials for Successful Server Consolidation." <http://www.compuware.com/dl/server.pdf>

¹⁷ "A blended threat is a computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods, for example using characteristics of both viruses and worms, while also taking advantage of vulnerabilities in computers, networks, or other physical systems. An attack using a blended approach might send a virus via an e-mail attachment, along with a Trojan horse embedded in an HTML file that will cause damage to the recipient computer. The Nimda, CodeRed, and Bugbear exploits were all examples of blended threats." http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci961251,00.html

¹⁸ "Worms Spread Faster, Blended Threats Grow." John Ledyden. October 1, 2003. The Register. http://www.theregister.co.uk/2003/10/01/worms_spread_faster_blended_threats/

¹⁹ 2004 CSI/FBI Computer Crime and Security Survey. Page 8.

“Opening IT Security” is one of a number of 3Com white papers discussing ROI and other important issues confronting decision-makers in organizations. This paper was researched by and developed with Phormion Sales Tools, Inc., www.phormion.com.

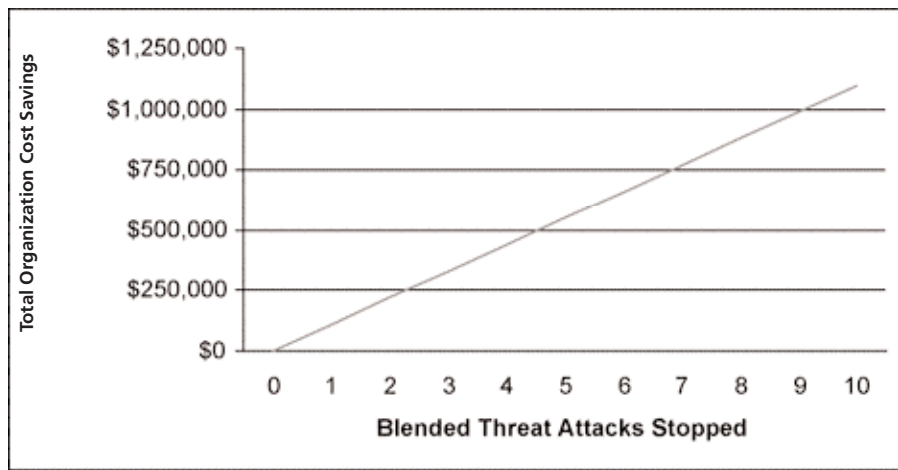


That same survey reported the cost of successful virus attacks (as calculated by the survey respondents) to be over \$204,000 per company per year, not including the cost of service denial, theft, fraud and a number of other cost categories. Similarly, a KPMG study in the UK put the cost of a single security breach at about \$110,000²⁰, while the UK’s Corporate IT forum estimates each security incident to cost nearly

\$175,000²¹. (Some estimates of per incident security breaches are outlandish: a poll in the 2002 timeframe placed the average security breach cost at \$2,000,000 per incident.)²²

Using the lowest of these estimates, Figure 4 illustrates the savings a more effective, integrated security system can provide by foiling attacks that may have otherwise penetrated the organization.

FIGURE 4: Annual Cost Savings Resulting From Improved Blended Threat Protection



Spending and Defending Smarter

Toward the end of 2002, the Meta Group reported that IT security budgets were increasing at a compounded annual growth rate of 40% to 50%²³; clearly, those writing the checks for the IT department had gotten the Security message.

Two years later, after several high-profile

worldwide virus and other attacks, there's no evidence the IT check writers are regretting those investments. But it's no secret that budgets are never unlimited, and good managers will always look for a more cost-effective way to solve their Security problem.

The 3Com Security Switch 6200 and Security Switch 7200 Family products is that solution.

20 “Cost of Each Security Breach - £77,000. IT Departments Struggling to Keep Up.” Andy McCue, vnunet.com. March 18, 2002. <http://www.networkitweek.co.uk/news/1130168>
 21 “Can ROI be Measured for Security Implementations?” August 10, 2004. Fran Howarth. <http://www.it-director.com/article.php?articleid=12138>
 22 “New Legislation Placing Increased Strain on Enterprise Security Programs.” December 18, 2002). http://www.systems-world.de/id/8319/CMEntries_ID/8268
 23 “New Legislation Placing Increased Strain on Enterprise Security Programs.” Systems-world.de. December 18, 2002. http://www.systems-world.de/id/8319/CMEntries_ID/8268

3Com Corporation, Corporate Headquarters, 350 Campus Drive, Marlborough, MA 01752-3064

To learn more about 3Com solutions, visit www.3com.com. 3Com is publicly traded on NASDAQ under the symbol COMS.

The information contained in this document represents the current view of 3Com Corporation on the issues discussed as of the date of publication. Because 3Com must respond to changing market conditions, this paper should not be interpreted to be a commitment on the part of 3Com, and 3Com cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only; 3Com makes no warranties, express or implied, in this document.

Copyright © 2004 3Com Corporation. All rights reserved. 3Com and the 3Com logo are registered trademarks of 3Com Corporation. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.

