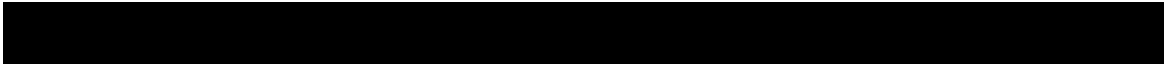


Reducing Downtime Costs with Network-Based IPS

April 2007





Copyright © 2007 by Infonetics Research, Inc.

Entire contents copyrighted by Infonetics Research, Inc. Unauthorized redistribution, electronic or otherwise, without prior written approval of Infonetics Research, Inc., is prohibited by law. Requests for permission to copy or distribute should be made to Infonetics Research, Inc.

Table of Contents

- I. Security Downtime Cost Overview1**
 - A. Introduction 1
 - B. Security Downtime Costs2
- II. Using Network-Based IPS to Reduce Security Downtime Cost.....4**
- III. Security Downtime Cost Analyzer6**
- Appendix7**
 - A. Revenue Loss Calculations7
 - B. Productivity Loss Calculations8

List of Exhibits

Exhibit 1	Security Downtime Costs	3
Exhibit 2	Security Downtime Costs by Source	4

I. Security Downtime Cost Overview

A. Introduction

Every year the CSI/FBI computer crime survey contains data about organization losses due to security breaches; respondents to that study report lost assets due to cybercrime, and past surveys have shown average losses in the hundreds of thousands of dollars per organization. In recent years, lost productivity and compliance issues have popped up as key drivers for investing in security solutions in addition to preventing theft of critical data.

This is a significant shift when thinking about security, risk, and the drivers for investing money in protection against electronic threats. For organizations to invest in security solely because of the threat of data loss or compromise, the primary requirement was to have valuable data running across their networks, as well as an understanding of the cost of the loss of that data. When this was the only driver for investing in security, security spending came from a small and paranoid subset of organizations worldwide.

Increased regulatory and compliance pressure (over the last 5 years or so) has broadened the potential audience for security investment to regulated vertical markets. Broad regulations like GLBA affect all public companies, and therefore increase the impact of regulatory pressure on security spending.

The true equalizer is downtime. All sizes and types of organizations around the globe experience downtime due to successful attacks. But what is the impact of those threats? How much does that downtime cost organizations? This paper gives an overview of how companies of all sizes are affected by security downtime, and discusses how implementing network-based IPS can drastically reduce the costs associated with security downtime.

B. Security Downtime Costs

We'll be looking at revenue and employee productivity losses due to DoS attacks and malware affecting clients, servers, and the network. We investigate 2 types of service interruption:

- Degradation—when a service is slower than usual, perhaps to the point of being useless, and
- Outages—when a service is unavailable

The second is usually more serious than the first, although both cause productivity losses.

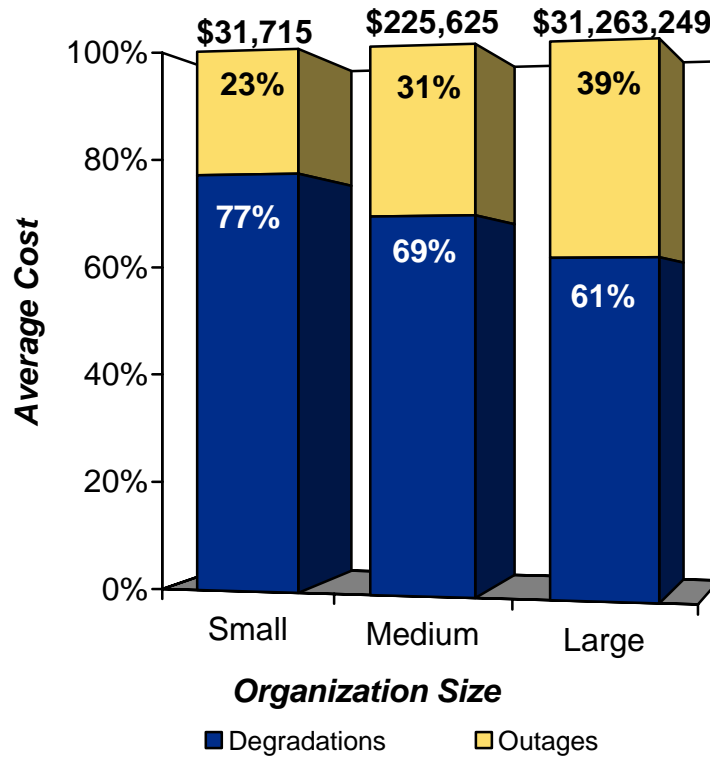
To calculate a per-organization average total of revenue and productivity losses due to security attack downtime, as well as the biggest culprits of the outages and degradations leading to downtime, we employ metrics gathered from respondents to an Infonetics study. In the study, titled *The Costs of Network Security Attacks: North America 2007*, we interviewed 80 small, 80 medium, and 80 large organizations regarding their security downtime. This approach allows us to use information that organizations are readily able to supply—numbers and durations of outages and service degradations due to attacks, annual organization revenue, etc. We are then able to use the information to estimate revenue and productivity losses, information that organizations aren't as likely to have at the ready. The exhibits and discussion in this chapter run the downtime calculations using the averages for each size group we interviewed. The appendix at the end of this paper describes the downtime calculations in detail.

The chart below shows the average per-organization annual cost of security downtime due to lost revenue and lost productivity for small, medium, and large organizations. Total security downtime cost for small organizations is just over \$30K (0.4% of revenue), with medium organizations topping \$225K (0.5% of revenue) and large organizations passing \$30M (2.2% of revenue). The chart shows downtime cost split between actual outages and service degradations. Downtime costs due to degradations are higher than those due to outages, primarily due to the fact that there are simply many more overall hours of degraded service than actual outage time. Also, though systems aren't

completely offline, performance is poor enough that the impact on employee productivity is similar.

Exhibit 1

Security Downtime Costs



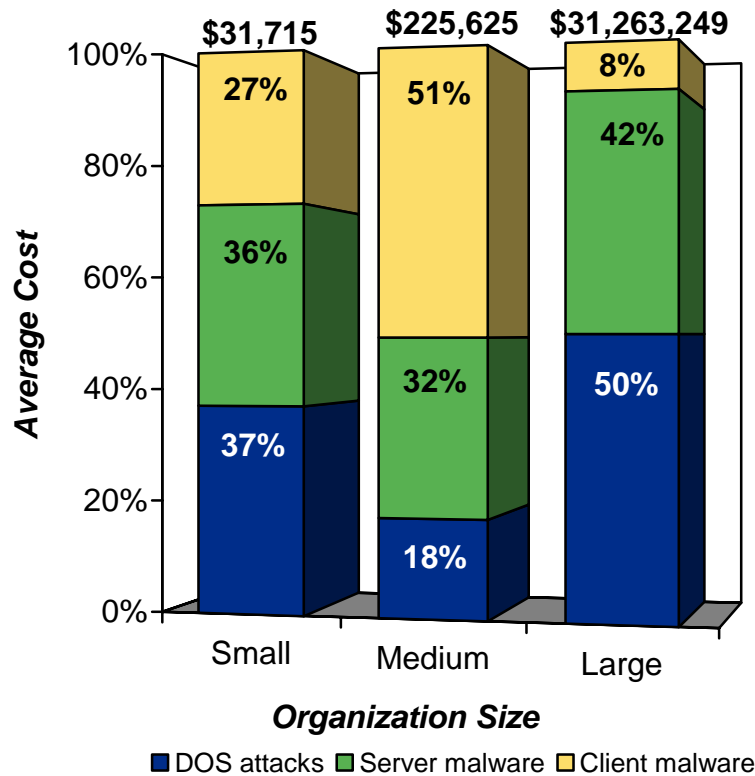
Source: The Costs of Network Security Attacks: North America 2007 (Infonetics Research)

In past network downtime research, we’ve noted that lost productivity due to service degradations is “hidden downtime,” meaning it often goes unreported (and therefore unfixed) for a long time. In many cases, it takes close monitoring of system and network performance to identify service degradations as quickly as possible and limit their impact.

Next we’ll look at the source of the problem: DOS attacks, client malware, and server malware, which paints an interesting picture. The results vary significantly by the size of the organization. Small organizations report roughly equal impact, medium organizations are most vexed by client malware, and large organizations have client malware largely in check, but are plagued roughly evenly by DOS attacks and server malware. It is important to mention

that large organizations, in most cases, have the best infrastructure in place to track downtime. Large organizations are also the focus of the most targeted attacks (including many targeted server/application and DOS attacks), whereas small and medium organizations are most impacted by indiscriminant attacks (mostly malware).

Exhibit 2 **Security Downtime Costs by Source**



Source: The Costs of Network Security Attacks: North America 2007 (Infonetics Research)

II. Using Network-Based IPS to Reduce Security Downtime Cost

Clearly most organizations will see decreases in downtime and downtime costs as they increase their investments in security technology. The question is, how much? Where is the balancing point? There is a wide array of products aimed at

protecting networks and systems from threats—from client-based solutions (anti-virus, personal firewalls, host IPS) to network-based solutions (firewalls, IDS, content security gateways, and IPS systems). All of these cover some threats, but the focus of this section is network-based IPS.

Network-based IPS devices are proactive security solutions that are deployed in the network. They look roughly like any other security appliance (however, with higher port densities), with some even resembling Ethernet switches. They are in-line devices, meaning that traffic is flowing through them in real-time. Some network IPS devices are purpose-built, like switches and routers, while some are PC-based. Most network IPS solutions are designed to use a variety of detection mechanisms (signatures, analysis of protocols and protocol anomalies, aberrations in traffic patterns, and a variety of other proprietary methods) to identify and block all types of malicious traffic. Network-based IPS solutions are designed to protect clients, servers, and network infrastructure from attacks of all types, including DOS/DDOS attacks, malware, worms, Trojans, and application specific threats. As a result, they are a good starting point for implementing comprehensive network security.

Based on real-world attack data provided by a variety of IPS vendors, as well as publicly available IPS test data, Infonetics Research has estimated how organizations can benefit by deploying proactive network-based IPS. This data shows that organizations who have not yet deployed network-based IPS will see roughly the following gains when moving to implement network-wide network-based IPS:

- **DOS attacks:** 65% reduction in downtime hours
- **Server malware:** 50% reduction in downtime hours
- **Client malware:** 40% reduction in downtime hours

These numbers will obviously vary based on the vendor selected, the number and variety of threats the IPS system is set to block, and the architecture of the network. However, we believe these numbers give a good rough idea of gains an average organization can expect to see.

DOS attacks are the least varied of the group, and most IPS products can detect and block DOS attacks with relative ease. Server and client malware both see a

significant decrease in downtime once network-based IPS devices are deployed. Downtime from DOS attacks, however, experiences the greatest decrease. This is due to the following: there are significantly more client/server malware attacks to detect (a simple numbers game), and there are times when clients (particularly laptops) are outside the reach of network-based IPS systems (while users are traveling and using public or guest networks).

III. Security Downtime Cost Analyzer

As a companion to this paper, we provide our *Security Downtime Cost Analyzer* (available in Excel format). This cost analyzer has 2 purposes:

- To help quantify your total downtime cost related to security threats and attacks
- To show the reduction in downtime cost after network-wide IPS is deployed

It is important to remember that we're simply showing the cost advantages of investing in network IPS to proactively reduce downtime. Infonetics makes no presumptions about the cost of lost data itself, nor do we factor in the impact of successful security breaches on regulations or compliance (i.e., fines due to insufficient protection, or the inability to operate because poor security stops the business licensing or insurance process).

To use the cost analyzer, simply open the Excel file and follow the instructions on the first sheet.

In many cases, the cost of purchasing new security solutions can be justified based on their impact on downtime alone—in the absence of thought about risk of loss or compliance exposure. This is something we think few organizations consider when working with corporate executives to understand risk and establish IT security budgets.

Appendix

A. Revenue Loss Calculations

As particular employees directly generate revenue, security attack downtime impacts corporate revenue. To calculate the effects is not an exact science, but by applying some reasonable assumptions, we can derive a good estimate that can be used to justify the expense and effort involved deploying solutions that stop or limit downtime due to security attacks.

In our **revenue** loss calculation, we use 4 key pieces of information:

- Total hours per year of outages and service degradations due to each of the types of security downtime (DOS attacks, client malware, and server malware), as reported by our respondents
- Total number of revenue-generating employees affected by outages or service degradations (calculated from the total number of employees per organization, and the percent of revenue-generating employees that are affected by outages and degradations)
- Average percent of productivity lost by revenue-generating employees during outages and degradations, as reported by our respondents
- Average annual revenue generated by each revenue-generating employee (calculated from the annual revenue per organization and the number of revenue-generating employees)

The **revenue** loss calculation is:

- Multiply the amount of revenue generated per revenue-generating employee per hour by the number of revenue-generating employees that are affected by outages or degradations; then multiply the result by the percent of productivity lost by revenue-generating employees during outages or degradations; this gives us the amount of revenue lost per hour of outages or degradations due to DOS attacks and malware
- Multiply the above by the annual length (in hours) of outages or degradations to find annual revenue loss

B. Productivity Loss Calculations

When a user is unable to use their computer or access network resources their productivity decreases significantly. This lost productivity has a direct impact on an organization's bottom line. Organizations of all sizes invest heavily in products that help boost their productivity, but often forget about solving systems problems that limit productivity.

In our **productivity** loss calculation, we use 4 key pieces of information:

- Total hours per year of outages and service degradations due to each of the types of security downtime (DOS attacks, client malware, and server malware), as reported by our respondents
- Total number of employees affected by outages or service degradations (calculated from the number of employees at respondent organizations, and the percent of employees affected by outages and degradations)
- Weighted average hourly wage per employee (calculated from the national average wages of clerical, professional, and executive employees, weighted by the average proportions of employee types at sites within respondent organizations, and by a loading factor that takes additional costs of employees into account)
- Average percent of productivity lost by employees during outages and service degradations, as reported by our respondents

The **productivity** loss calculation is:

- To find productivity lost by revenue-generating employees, multiply the weighted hourly wage per employee by the number of revenue-generating employees affected by outages or degradations; multiply the result by the percent of productivity lost by revenue-generating employees during outages or degradation; finally, multiply the result by number of annual hours of outages or degradations
- To find productivity lost by non-revenue-generating employees, multiply the weighted hourly wage per employee by the number of non-revenue-generating employees affected by outages or degradations; multiply the result by the percent of productivity lost by non-revenue-generating employees during outages or degradations; finally, multiply the result by number of annual hours of outages or degradations
- To find total cost of productivity loss by all employees, sum the above

About Infonetics Research

Infonetics Research (www.infonetics.com) is the premier international market research and consulting firm specializing in data networking and telecom. We provide a complete view of the market through constant interaction with equipment manufacturers, service providers, end-users, chip and component manufacturers, sales channels, and the financial community. We offer quarterly market share and forecasting, end-user survey research, service provider survey research, and service provider capex analysis. We are respected in the industry for being objective and accurate and for delivering on time all the time.

Services

- Market Share, Market Size & Forecasts
- End-User & Service Provider Survey Research
- Service Provider Capex Analysis & Forecasts
- Consulting, Retainers & Quick Consults
- Webinar, Conference & Event Speaking
- Custom Demand-Side & Brand Market Research
- Custom Market Size & Forecasts
- Technology and White Papers
- Competitive Analysis & Due Diligence

Coverage Areas

- Broadband & IPTV
- Enterprise Voice & Data
- Network Security
- Service Provider Capex
- Service Provider Optical, Metro E, Routing & Switching
- Service Provider VoIP, IMS & FMC
- Total Telecom & Datacom
- Wireless & FMC

Contact Information

US Headquarters

900 East Hamilton Ave #230
Campbell, CA 95008
United States
t +1 408.583.0011
f +1 408.583.0031

Boston Metro Office

3 Baldwin Green Common #307
Woburn, MA 01801
United States
t +1 781.933.9649
f +1 781.933.9659

London Office

P.O. Box 629
Bromley, Kent BR1 4WB
United Kingdom
t + 44 168.985.1618
f + 44 168.985.1618

Sales

Larry Howard, Vice President

larry@infonetics.com
t +1 408.583.3335
f +1 408. 583.0031