

The Return on Investment for Network Security

The fourth in a series entitled *Network Security Investment—The Executive ROI Briefcase*, this white paper helps executives understand the value of network security with regard to the economic consequences of a security breach.

Other white papers in the series include:

- Economic Impact of Network Security Threats

This white paper describes the dynamics in today's business climate that are driving network security requirements, and provides an understanding of the threats facing business leaders today.

- Privacy Protection Depends on Network Security

This white paper reviews some of the laws that mandate consumer privacy protection and how network security helps ensure data privacy.

- Recovery After a Breach in Network Security

This white paper discusses best practices for disaster recover that involve information security and IT professionals, as well as law enforcement

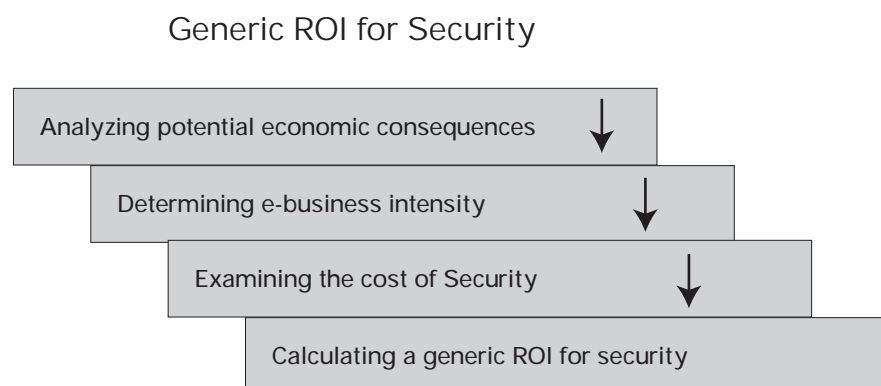
- Action Steps for Improving Information Security

This white paper describes the steps you should take to ensure a secure network infrastructure.

Executive Summary

Many organizations prefer to take a generic approach to evaluating return on investment (ROI) for network security activities and processes Independent research firm Computer Economics has assembled data for several years that can help organizations with a well-structured generic ROI analysis. Working with generic data still requires several steps, shown in the flowchart depicted in Figure 1.

Figure 1
Steps to Determine ROI for Security



Analyzing Potential Economic Consequences

Organizations face three types of economic impact as a result of hacks or intrusions. The immediate economic impact is the cost of repairing or replacing systems and the disruption of business operations and cash flow. Short-term economic impact on an organization includes the loss of contractual relationships or existing customers because of the inability to deliver products or services and a negative impact on the reputation of the organization. Long-term economic impact includes the decline in an organization's market valuation and stock prices. Types of economic impact of malicious attacks on an organization are shown in Table 1.

Table 1

Types of Economic Impact of Hack Attacks on an Organization

Type of Economic Impact on Organizations	Consequences of Impact
Immediate economic impact on a single organization	<ul style="list-style-type: none">• Damage to systems that require human intervention to repair or replace• Disruption of business operations• Delays in transactions and cash flow
Short-term economic impact on a single organization	<ul style="list-style-type: none">• Loss of contractual relationships with other organizations in supply chains• Loss of retail sales• Negative impact on the reputation of an organization• Hindrance to the development of new business
Long-term economic impact on a single organization	<ul style="list-style-type: none">• Decline in market valuation• Erosion of investor confidence• Decline in stock price• Reduced goodwill standing

Source: *Computer Economics*

Computer Economics has studied the economic impact of malicious attacks on organizations for several years. Table 2 shows the average economic impact of malicious attacks that can be expected to occur if adequate security protection is not implemented. The greater the dependence on e-business technology, the greater the economic impact of malicious attacks. The quantity of nodes in the table refers to any device that is attached to the network.

Table 2

Annual Economic Impact of Malicious Attacks

Number of Nodes	Economic Impact on a Low-Intensity e-Business Company	Economic Impact on a Medium-Intensity e-Business Company	Economic Impact on a High-Intensity e-Business Company
25	\$12,025	\$31,085	\$66,138
50	\$25,200	\$61,589	\$131,040
100	\$46,674	\$109,684	\$233,370
250	\$108,375	\$239,401	\$509,363
500	\$203,600	\$430,614	\$916,200
1,000	\$402,225	\$812,897	\$1,729,568
2,000	\$787,350	\$1,554,229	\$3,306,870
3,000	\$1,244,970	\$2,399,057	\$5,104,377
5,000	\$2,243,875	\$4,113,023	\$8,751,113
10,000	\$4,065,416	\$6,878,684	\$14,635,498
20,000	\$7,231,488	\$11,555,918	\$24,587,059
50,000	\$16,789,500	\$25,251,408	\$53,726,400

Source: *Computer Economics*

These projections are modeled from five years of historical data and include the costs of cleaning systems infected by malicious code, the recovery costs from hack attacks and intrusions, lost revenue, and loss of productivity of employees. The economic impact of attacks varies with the level of systems security. The greater the security, the less annual economic impact.

The total economic impact can be divided into several subcategories. The lion's share of the economic impact of malicious attacks is in lost revenue. In smaller companies, lost revenue accounts for about 50 percent of the economic impact. However, in larger companies, lost revenue represents about 80 percent of the total economic impact.

The cost of cleaning, repairing, and restoring computers and networks represents about 20 percent of the economic impact in smaller companies and eight percent in larger companies. The loss of productivity represents about 30 percent in smaller companies and 12 percent in larger companies.

Determining E-Business Intensity

Your company may already be high-intensity if the majority of your revenue is generated through Web-based or supply-chain applications. If you don't fit into this category, however, it is critical that you consider where your business is going. Today, you may not be Web-based or use supply-chain applications for revenue generation, but you may be moving in that direction and in the future you could be more dependent on these sources of revenue. If so, you will need better security in place as you move ahead. Factors considered in assessing your e-business intensity include the following:

- *Information systems staffing mix*—Sectors and organizations that have more than the average number of e-commerce application developers in their IT departments rank higher in e-business intensity. Organizations that have fewer than the average number of e-commerce applications developers in their IT departments rank lower in e-business intensity.
- *E-commerce software in place*—Sectors and organizations that have e-commerce software in place rank higher in e-business intensity, while those organizations that do not have e-commerce software in place rank lower.
- *Plans to buy e-commerce software*—Sectors and organizations that have plans to buy e-commerce software rank higher in e-business intensity, while those organizations that do not have plans to buy e-commerce software rank lower.

- *Web site*—Sectors and organizations with Web sites rank higher in e-business intensity, while those organizations that do not have Web sites rank lower.
- *Internet connectivity*—Sectors and organizations with Internet connectivity rank higher in e-business intensity while those organizations that do not have Internet connectivity rank lower.
- *Telecommuting*—Sectors and organizations that support telecommuting capabilities with IT rank higher in e-business intensity. Organizations that do not support telecommuting capabilities with IT rank lower in e-business intensity.
- *Web-based business-to-business transactions*—Sectors and organizations that support Web-based business-to-business (B2B) transactions rank higher in e-business intensity, while those organizations that do not support Web-based B2B transactions rank lower.
- *Web-based business-to-consumer transactions*—Sectors and organizations that support Web-based business-to-consumer (B2C) transactions rank higher in e-business intensity, while those organizations that do not support Web-based B2C transactions rank lower.
- *Electronic data interchange via Web site*—Sectors and organizations that support electronic data interchange (EDI) via the Web rank higher in e-business intensity, while those organizations that do not support EDI via the Web rank lower.
- *EDI via direct-dial connections with suppliers*—Sectors and organizations that support EDI via direct-dial connections with suppliers rank higher in e-business intensity, while those organizations that do not support EDI via direct-dial connections with suppliers rank lower.
- *EDI via direct-dial connections with consumers*—Sectors and organizations that support EDI via direct-dial connections with consumers rank higher in e-business intensity, while those organizations that do not support EDI via direct-dial connections with consumers rank lower.

What Composes the Cost of Security?

Computer Economics has benchmarked the percent of IT budgets spent on security since 1990. The most recent study shows that the majority of organizations spend less than two percent of their IT budgets on security. In situations where system availability, data integrity, and confidentiality are extremely important, organizations spend as much as five percent of their IT budget on security.

The cost of deploying security is divided among many budget categories and varies considerably across organizations. Table 3 shows the average 2002 central information systems (IS) budget allocations and the level of spending on security products or activities that are generally charged to each major category. In low-threat environments, security spending is lower. In high-threat environments such as financial organizations, security spending is higher. The cost of security can be impacted by many circumstances, including size and nature of the business, government regulations, level of e-business intensity, and whether network management is outsourced or internally managed.

Table 3

Central IS Budget Allocations in 2002

Sectors	Average Percentage of IS Budget Allocated	Spending on Security Activities or Products
Mainframes	4.7	Moderate
Midrange systems	7.4	Moderate
LAN servers/superservers	8.7	High
Data network infrastructure	8.0	High
Workstations, desktop PCs, portables, and notebooks	8.7	High
Operating system and utility software	5.5	Moderate
Application software	6.8	Moderate
Outside services	5.7	Moderate
Personnel costs	36.0	High
Facilities and overhead	3.1	Low
Consumable supplies	2.3	Low
Training	3.0	Moderate
<i>Source: Computer Economics</i>		

The effort to deploy and maintain security is divided across many personnel functions and also varies across organizations. Table 4 shows the average 2002 IS staffing mix and the level of effort required to install and maintain security products and support security activities.

Table 4

IS Staffing Mix Across All Sectors in 2002

Job Function	Percent of IS Staff	Effort Spent on Security Activities
Data entry	1.4	Low
Systems operators	9.5	Low
Network administrators	9.7	High
PC technical support	6.3	High
Help desk	9.5	Moderate
Systems engineering	4.8	Moderate
Systems programmers	4.3	Moderate
Database administration	3.4	Low
Applications programmers	24.9	Low
Documentation specialists	1.5	Low
Quality assurance	2.5	Low
E-commerce staff	6.5	Moderate
Information systems managers/ administrators	9.3	Moderate
Clerical support	3.2	Low
Other	3.5	Low

Source: *Computer Economics*

Calculating a Generic ROI for Security

When examining the return on investment (ROI) for security spending several variables must be considered. The process of determining security expenditures takes into consideration existing expenditures as well what might be needed after threat levels are reevaluated.

To be considered first is the amount spent on security. In many cases this is difficult to determine, beyond what is known to be direct spending for security products and personnel time that is readily identifiable as a security expenditure. In organizations where good security systems are in place, there may be more data available.

Secondly, the existing threat level, or at least what is known about the existing threat level, must be established. It is important to recognize there is a consistent pattern of security breaches not always being reported.

Third, there are laws, regulations, and defense requirements that require certain types of organizations to take extra steps in protecting information systems from attack. Thus many organizations may need to spend beyond a break-even point, given the known threat level, in order to achieve legal, regulatory, or contractual compliance. In these cases a generalized ROI for security becomes academic-if the organization does not comply with requirements it will not be able to maintain business operations.

Break-Even Spending for IT Security

As a general guideline for evaluating spending levels for any IT equipment or software, a break-even point for ROI can be applied. However, as previously noted, organizations may face external requirements that change the break-even requirements. To calculate a basic annual break-even point, the economic impact from a substantiated threat is divided by the total number of nodes (see Table 5). The annual cost per node for security declines as the number of nodes increases because of the economy of scale in software licenses and the deployment of security products. The break-even costs include computer and network security.

Table 5

Annual Break-Even Spending for IT Security Per Node

Number of nodes in the organization	Break-even security spending per node for low intensity company	Break-even security spending per node for medium intensity company	Break-even security spending per node for high intensity company
25	\$230	\$342	\$376
50	\$232	\$338	\$376
100	\$228	\$335	\$374
250	\$225	\$336	\$374
500	\$233	\$336	\$393
1,000	\$254	\$336	\$448
2,000	\$225	\$336	\$396
3,000	\$224	\$337	\$398
5,000	\$223	\$337	\$401
10,000	\$221	\$335	\$400
20,000	\$181	\$303	\$323
50,000	\$219	\$267	\$403

Source: *Computer Economics*

Costs and ROI for Security

The cost for security products varies from organization to organization. For computer systems, typical security deployments, including antivirus and firewall products for small quantities of desktops, file servers, and application servers will cost from \$100 to \$300 per machine, with volume discounts resulting in a cost reduction of about 50 percent.

Protecting networks requires a broad mix of products, including technology to assure identity, manage perimeter security, enable secure connectivity, monitor security, and manage security policy. Cost for network security products range from \$25 per node in small organizations up to about \$85 per node for larger organizations. Product pricing will vary by vendor and by country.

In e-business-intensive organizations the potential economic impact of malicious attacks is much higher. This increases the need for security products and personnel. Tables 6 to 8 show the costs per node and the ROI for security products for organizations with different low, medium, and high levels of e-business intensity organizations.

Table 6

Annual Costs and ROI for Security in a Low Intensity E-Business Environment

Number of nodes in the organization	Projected costs for computer security products	Projected costs for network security products	Associated personnel costs	Total projected security costs	Economic impact of malicious attacks	ROI for security spending
25	\$2,500	\$987	\$2,256	\$5,743	\$12,025	\$6,282
50	\$5,200	\$1,974	\$4,418	\$11,592	\$25,200	\$13,608
100	\$9,900	\$4,160	\$8,742	\$22,802	\$46,674	\$23,873
250	\$23,300	\$11,045	\$21,902	\$56,247	\$108,375	\$52,128
500	\$45,900	\$22,490	\$48,236	\$116,626	\$203,600	\$86,975
1,000	\$81,200	\$75,200	\$97,297	\$253,697	\$402,225	\$148,528
2,000	\$148,500	\$106,455	\$195,826	\$450,781	\$787,350	\$336,569
3,000	\$207,800	\$166,709	\$297,416	\$671,925	\$1,244,970	\$573,045
5,000	\$324,800	\$287,969	\$500,973	\$1,113,742	\$2,243,875	\$1,130,133
10,000	\$617,200	\$591,166	\$999,925	\$2,208,291	\$4,065,416	\$1,857,125
20,000	\$1,100,000	\$763,750	\$1,750,750	\$3,614,500	\$7,231,488	\$3,616,988
50,000	\$2,784,000	\$3,097,300	\$5,070,360	\$10,951,660	\$16,789,500	\$5,837,840

Source: Computer Economics

Table 7

Annual Costs and ROI for Security in a Medium Intensity E-Business Environment

Number of nodes in the organization	Projected costs for computer security products	Projected costs for network security products	Associated personnel costs	Total projected security costs	Economic impact of malicious attacks	ROI for security spending
25	\$2,500	\$1,250	\$4,800	\$8,550	\$31,085	\$22,535
50	\$5,200	\$2,300	\$9,400	\$16,900	\$61,589	\$44,689
100	\$9,900	\$4,950	\$18,600	\$33,450	\$109,684	\$76,234
250	\$23,300	\$14,200	\$46,600	\$84,100	\$239,401	\$155,301
500	\$45,900	\$29,000	\$93,300	\$168,200	\$430,614	\$262,414
1,000	\$81,200	\$68,700	\$186,500	\$336,400	\$812,897	\$476,497
2,000	\$148,500	\$151,300	\$372,000	\$671,800	\$1,554,229	\$882,429
3,000	\$207,800	\$242,200	\$560,000	\$1,010,000	\$2,399,057	\$1,389,057
5,000	\$324,800	\$425,100	\$935,000	\$1,684,900	\$4,113,023	\$2,428,123
10,000	\$617,200	\$880,000	\$1,850,000	\$3,347,200	\$6,878,684	\$3,531,484
20,000	\$1,100,000	\$1,225,000	\$3,725,000	\$6,050,000	\$11,555,918	\$5,505,918
50,000	\$2,784,000	\$4,250,000	\$6,300,000	\$13,334,000	\$25,251,408	\$11,917,408

Source: Computer Economics

Table 8

Annual Costs and ROI for Security in a High Intensity E-Business Environment

Number of nodes in the organization	Projected costs for computer security products	Projected costs for network security products	Associated personnel costs	Total projected security costs	Economic impact of malicious attacks	ROI for security spending
25	\$2,500	\$2,100	\$4,800	\$9,400	\$66,138	\$56,738
50	\$5,200	\$4,200	\$9,400	\$18,800	\$131,040	\$112,240
100	\$9,900	\$8,850	\$18,600	\$37,350	\$233,370	\$196,020
250	\$23,300	\$23,500	\$46,600	\$93,400	\$509,363	\$415,963
500	\$45,900	\$47,850	\$102,630	\$196,380	\$916,200	\$719,820
1,000	\$81,200	\$160,000	\$207,015	\$448,215	\$1,729,568	\$1,281,353
2,000	\$148,500	\$226,500	\$416,650	\$791,650	\$3,306,870	\$2,515,220
3,000	\$207,800	\$354,700	\$632,800	\$1,195,300	\$5,104,377	\$3,909,077
5,000	\$324,800	\$612,700	\$1,065,900	\$2,003,400	\$8,751,113	\$6,747,713
10,000	\$617,200	\$1,257,800	\$2,127,500	\$4,002,500	\$14,635,498	\$10,632,998
20,000	\$1,100,000	\$1,625,000	\$3,725,000	\$6,450,000	\$24,587,059	\$18,137,059
50,000	\$2,784,000	\$6,590,000	\$10,788,000	\$20,162,000	\$53,726,400	\$33,564,400

Source: *Computer Economics*

Summary

Being able to calculate your return on investment helps you make important decisions with regard to network security. With a secure foundation for information sharing, you can increase your revenue through e-business and benefit from an increase in the productivity of your employees. Learn what steps to take to ensure a secure network through the fifth white paper in this series, *Action Steps for Improving Information Security*.

Other white papers in the series include:

- Economic Impact of Network Security Threats

This white paper describes the dynamics in today's business climate that are driving network security requirements, and provides an understanding of the threats facing business leaders today.

- Privacy Protection Depends on Network Security

This white paper reviews some of the laws that mandate consumer privacy protection and how network security helps ensure data privacy.

- Recovery After a Breach in Network Security

This white paper discusses best practices for disaster recover that involve information security and IT professionals, as well as law enforcement.

You can find this series of white papers, design and implementation guides, and case studies that demonstrate how other companies implemented security and VPN solutions over a secure network to expand connectivity and reduce costs at <http://www.cisco.com/go/security>.

About Computer Economics' Methodology

Independent research firm Computer Economics has collected and analyzed data on the impact of malicious code attacks, hacking and intrusion incidents, and the cost of system downtime for several years. Much of this work dates back as far as the early 1990s. The analysis of malicious code attacks intensified in the late 1990s as major virus incidents such as Melissa, I Love You, Code Red, and Nimda became commonplace.

The research has largely been client-driven. When Computer Economics' clients needed to determine the ROI for security and virus protection, an in-depth research process was initiated. Data collection is ongoing and involves the following:

- Reviewing numerous statistical reports and studies on computer crime and malicious attacks of all sorts
- Collecting data on the economic aspects of malicious attacks
- Benchmarking cleanup and recovery costs from major incidents
- Benchmarking the impact on productivity that attacks have on different types of organizations
- Benchmarking lost revenue from downtime

- Monitoring the activity reports of security companies, including the frequency of different types of attacks and the recurrence of virus activity
- Conducting ongoing surveys of IT spending, security practices, and the cost of malicious attacks

The economic impact analysis and models that Computer Economics creates are based on numerous research efforts over a period of several years. Data has been obtained from more than 2000 organizations from virtually every industry sector and every major industrial country around the world.

The analyst teams for these projects have been led by Michael Erbschloe, vice president of research for Computer Economics of Carlsbad, California. Mr. Erbschloe is the author of *Information Warfare: How to Survive Cyber Attacks* and *The Executive's Guide to Privacy Management*. He also coauthored *Net Privacy: A Guide to Developing & Implementing an Ironclad ebusiness Privacy Plan*. In addition, he has presented at professional conferences around the world.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: 65 317 7777
Fax: 65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)