INPUT®

RESEARCH REPORT

Evaluation of Security Solutions for Electronic Commerce, U.S.

FC37U

Evaluation of Security Solutions for Electronic Commerce, U.S.

INPUT®

Frankfurt • London • New York • Paris • San Francisco • Tokyo • Washington D.C.

INPUT®

Clients make informed decisions more quickly and economically by using INPUTs' services. Since 1974, information technology (IT) users and vendors throughout the world have relied on INPUT for data, research, objective analysis and insightful opinions to prepare their plans, market assessments and business directions, particularly in computer software and services.

Contact us today to learn how your company can use INPUT's knowledge and experience to grow and profit in the revolutionary IT world of the 1990s.

Subscription Services

- Information Services Markets
  - Worldwide and country data
  - Vertical industry analysis
- Business Integration Markets
- Systems Integration and Professional Services Markets
- Client/Server Software Platforms
- Outsourcing Markets
- Information Services Vendor Profiles and Analysis
- Electronic Commerce/Internet
- U.S. Federal Government IT Markets
- IT Customer Services Directions (Europe)

Service Features

- Research-based reports on trends, etc. (Over 100 in-depth reports per year)
- Frequent bulletins on events, issues, etc.
- 5-year market forecasts
- Competitive analysis
- Access to experienced consultants
- Immediate answers to questions
- On-site presentations

Databases

- Software and Services Market Forecasts
- Software and Services Vendors
- U.S. Federal Government
  - Procurement Plans (PAR)
  - Forecasts
  - Awards (FAIT)
  - Agency Procurement Requests (APR)

Custom Projects

For Vendors–analyse:

- Market strategies and tactics
- Product/service opportunities
- Customer satisfaction levels
- Competitive positioning
- Acquisition targets

For Buyers–evaluate:

- Specific vendor capabilities
- Outsourcing options
- Systems plans
- Peer position

Other Services

Acquisitions/partnerships searches

INPUT Worldwide

Frankfurt
Perchstätten 16
D-35428 Langgöns
Germany
Tel: +49 (0) 6403 911420
Fax: +49 (0) 6403 911413

London
Cornwall House
55-77 High Street
Slough, Berkshire
SL1 1DZ UK
Tel: +44 (0) 1753 530444
Fax: +44 (0) 1753 577311

New York
300 Frank W. Burr Blvd.
Teaneck, NJ 07666
U.S.A.
Tel: +1 (201) 801-0050
Fax: +1 (201) 801-0441

Paris
24, avenue du Recteur
Poincaré
75016 Paris
France
Tel: +33 (1) 46 47 65 65
Fax: +33 (1) 46 47 69 50

San Francisco
1881 Landings Drive
Mountain View
CA 94043-0848
U.S.A.
Tel: +1 (650) 961-3300
Fax: +1 (650) 961-3966

Tokyo
6F#B, Mitoshiro Building,
1-12-12, Uchikanda
Chiyoda-ku, Tokyo 101
Japan
Tel: +81 3 3864-0531
Fax: +81 3 3864-4114

Washington, D.C.
1921 Gallows Road
Suite 250
Vienna, VA 22182 3900
U.S.A.
Tel: +1 (703) 847-6870
Fax: +1 (703) 847-6872

Abstract

This report analyzes buyer behavior and attitude concerning electronic commerce security products and services purchased in the U.S. Fifty-two buyer companies were polled concerning their experiences and thoughts on a variety of security related issues. Their feedback forms the basis of this report, which is intended to:

- Help vendors to understand the relative importance of key security product features and needs.
- Provide vendors with insights into user implementations, plans and budgets.
- Help users to obtain perspective on what other security firms see as being major issues.
- Reveal how users perceive vendors.

Published by
INPUT
1881 Landings Drive
Mountain View, CA 94043-0848
United States

Electronic Commerce

Evaluation of Security Solutions for Electronic Commerce, U.S.

The information provided in this report shall be used only by the employees of and within the current corporate structure of INPUT's clients, and will not be disclosed to any other organization or person including parent, subsidiary, or affiliated organization without prior written consent of INPUT.

INPUT exercises its best efforts in preparation of the information provided in this report and believes the information contained herein to be accurate. However, INPUT shall have no liability for any loss or expense that may result from incompleteness or inaccuracy of the information provided.

PC37U • 1998 • 1014

Table of Contents

List of Exhibits

I.

II.

III.

IV.

V.

VI.

I

Introduction

A

Objectives and Scope

Electronic commerce is enabling companies to dramatically increase the speed of payments, reduce errors and paperwork, and improve productivity. Implementing electronic commerce systems requires extensive deployment of computers, networks and related software. This in turn has resulted in a wide variety of security solutions being implemented to help protect and prevent misuse of these systems.

There are literally hundreds of companies offering thousands of security products, ranging from virus detection to firewalls to public-key encryption. This study is intended to:

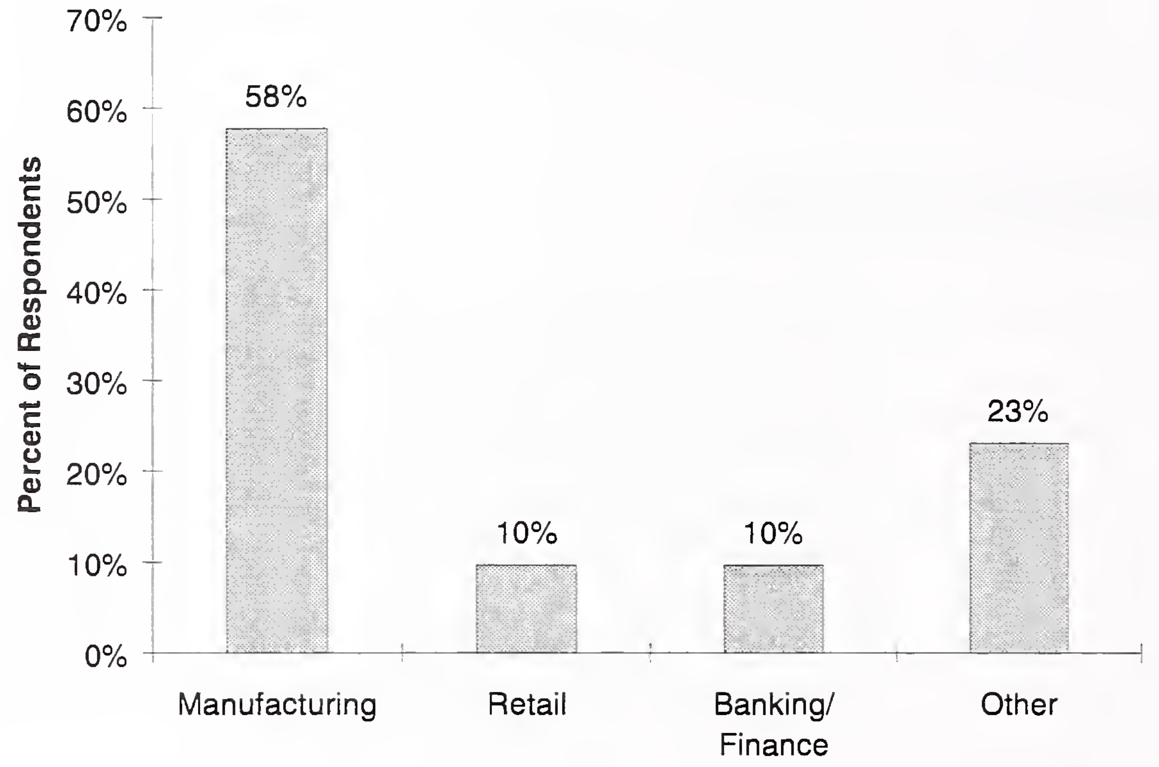
- Help vendors to understand the relative importance of key security product features and needs.
- Provide vendors with insights into user implementations, plans and budgets.
- Help users to obtain perspective on what other security firms see as being major issues.
- Reveal how users perceive vendors.

B
Research Methodology

INPUT interviewed 52 large U.S. companies during May 1998. Exhibit I-1 shows the sample breakdown by industry.

Exhibit I-1

Sample Breakdown by Industry



Number of Respondents: 52

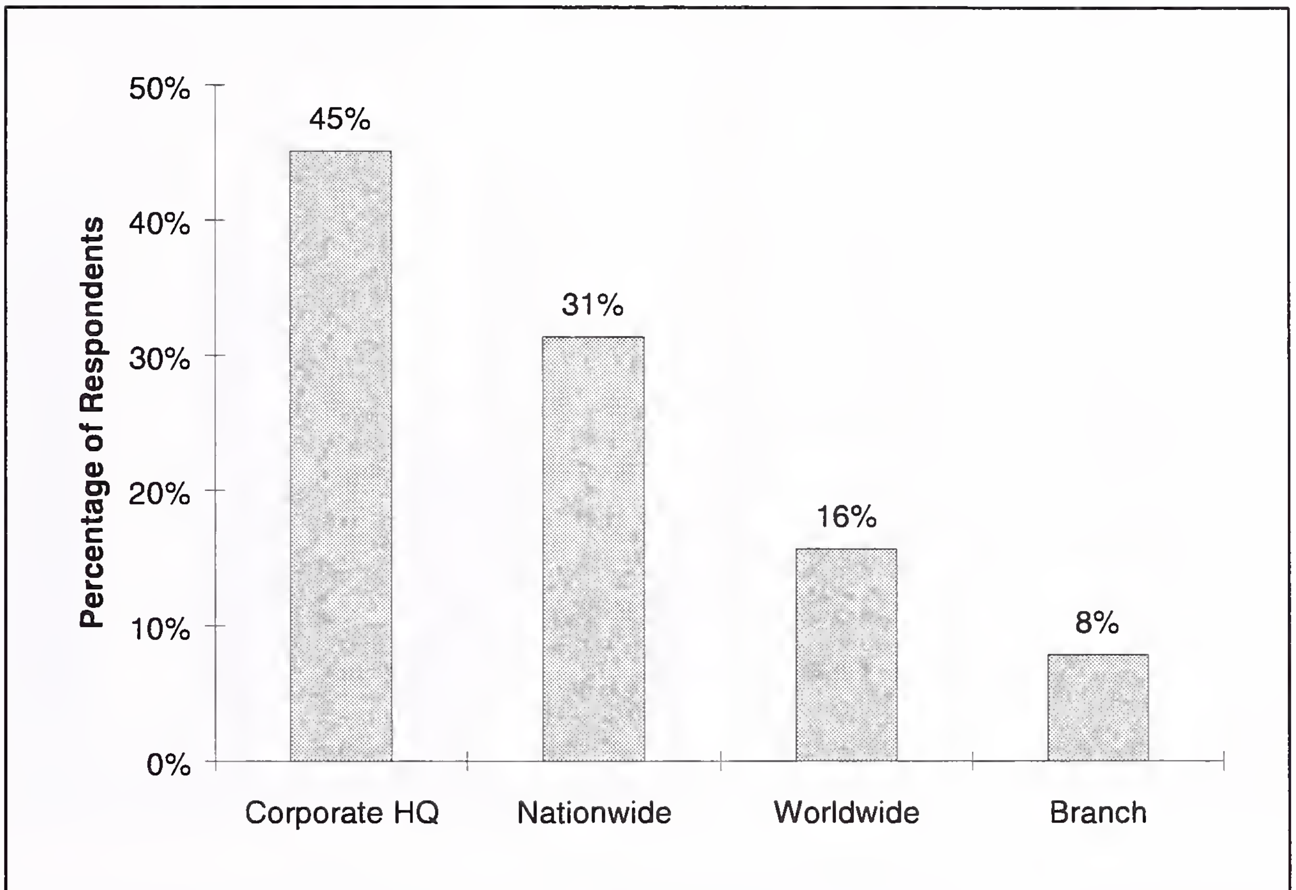
Source: INPUT

As one might expect, given their high use of EDI (electronic data interchange), manufacturing, finance and retail industry sectors accounted for 77% of the respondents interviewed.

Exhibit I-2 shows the sample breakdown by respondents' scope of responsibility.

Exhibit I-2

Sample Breakdown by Scope of Responsibility



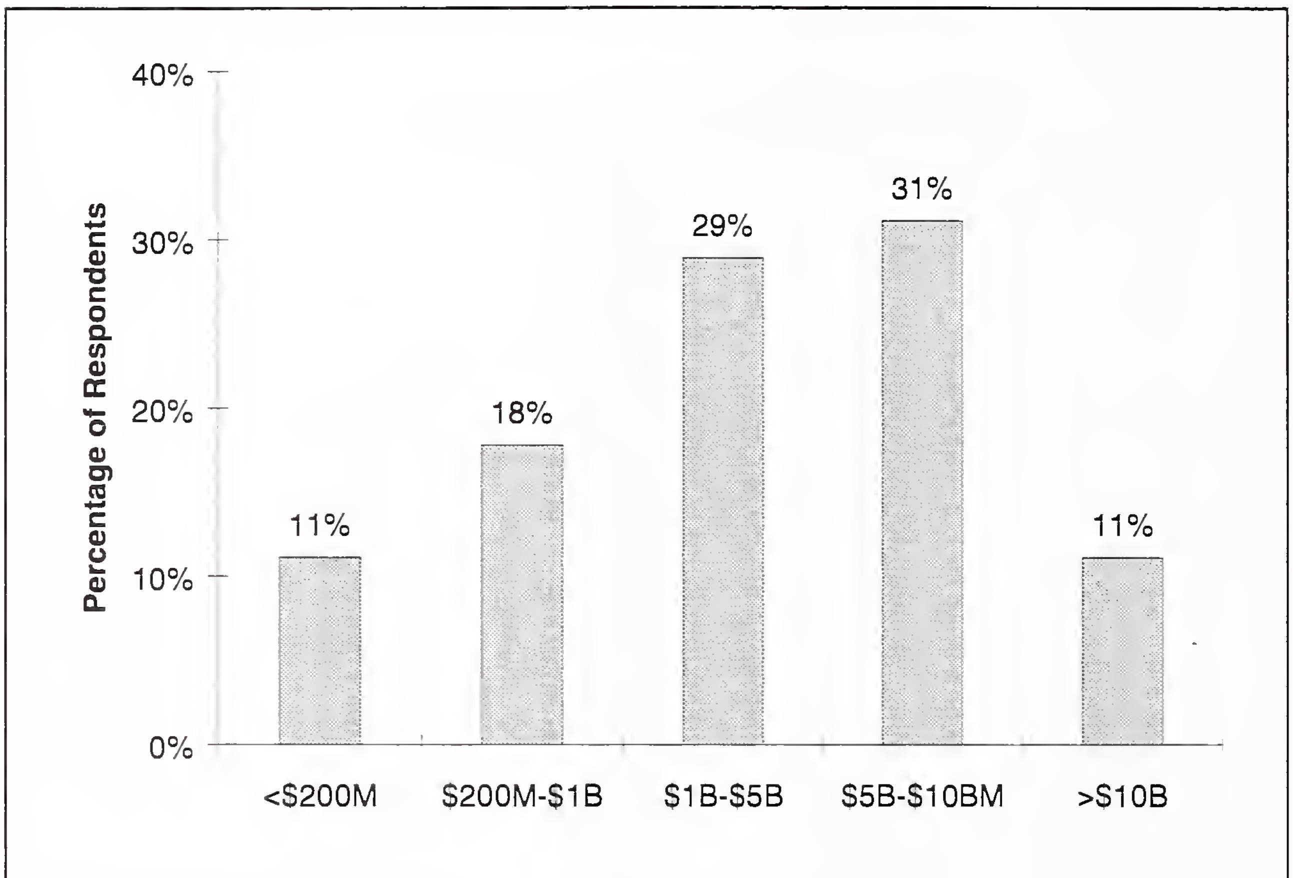
Number of Respondents: 51 *Source: INPUT*

In general, individuals responsible for aspects of electronic commerce security tend to be have corporate-wide responsibilities.

Exhibit I-3 shows the sample distribution by respondent company revenues.

Exhibit I-3

Sample Breakdown by Revenues



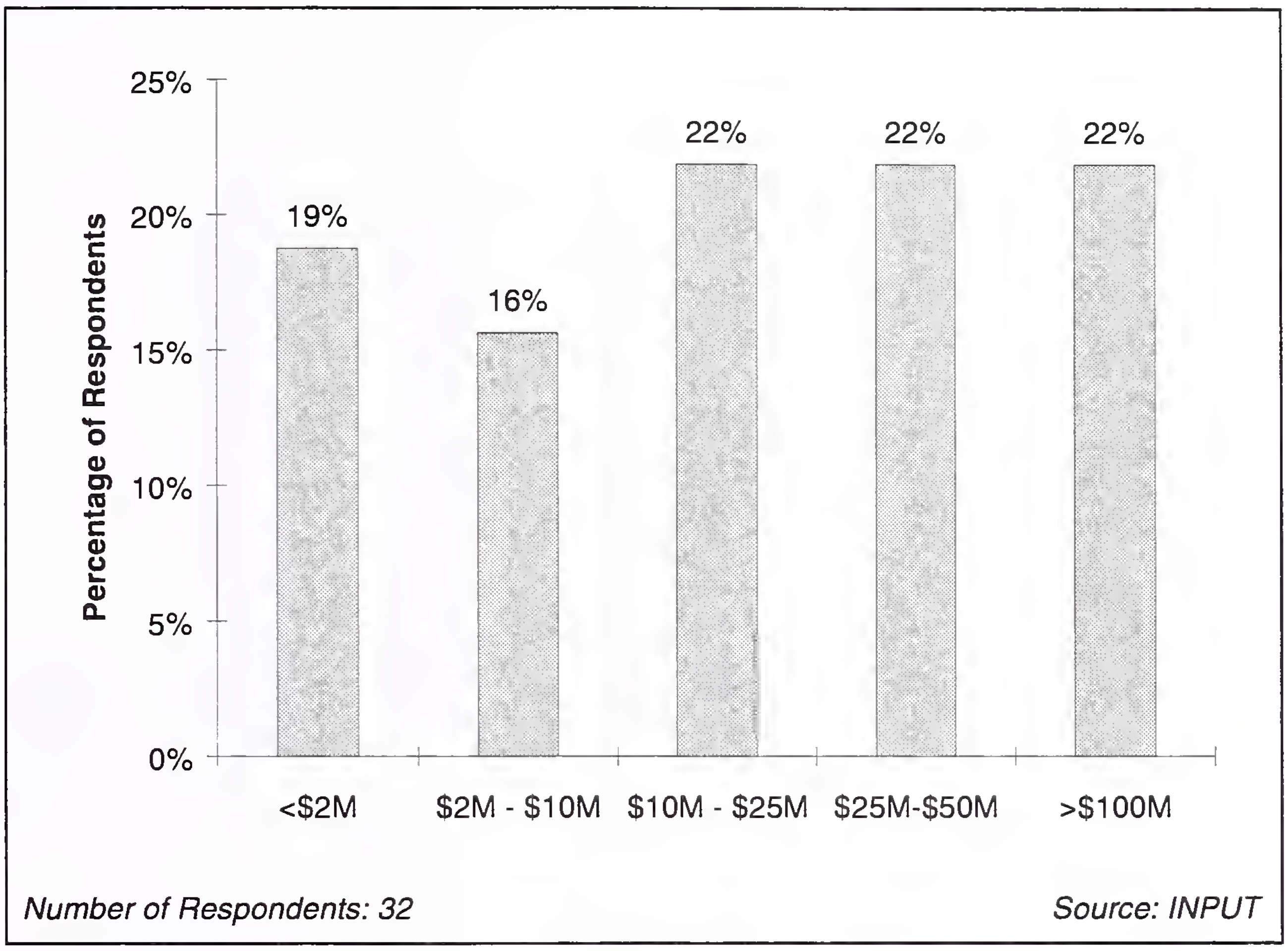
Number of Respondents: 45

Source: INPUT

In this report, a high percentage of the respondent companies made intensive use of EDI. Historically, due to the high cost of implementing EDI, such companies have needed to have substantial revenues before being able to justify such an expense.

Exhibit I-4

Sample Breakdown by IS Budget



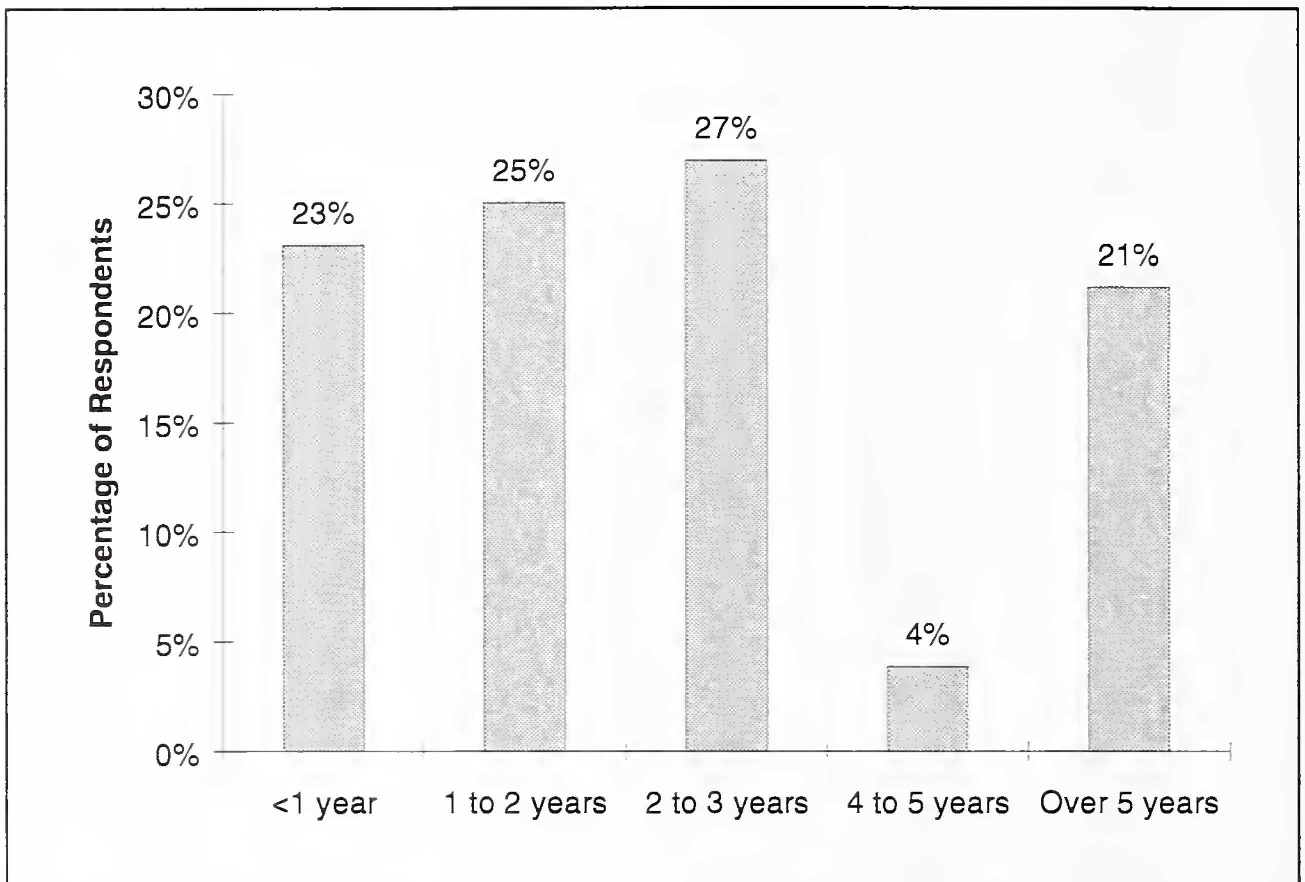
Number of Respondents: 32

Source: INPUT

The majority of respondents had IS budgets well over $10 million dollars. These budgets averaged 1.4% of company revenues and approximately 6% of this budget was spent on security.

Exhibit I-5

Breakdown of Respondent Experience in Electronic Commerce



Number of Respondents: 52

Source: INPUT

Only 25% of the respondents had over three years of experience in electronic commerce security. This is not surprising in this rapidly expanding area of specialization.

C
Report Structure

- Chapter II—Executive Summary, presents a summary of the key findings of this report. It identifies user perspectives on perceived risks, concerns and vulnerabilities associated with electronic commerce security, as well as their objectives and plans. Key vendors are identified, and overall implications for users and vendors are summarized.

- Chapter III— Usage of Electronic Commerce and Security Products and Services, examines how users are using electronic commerce security, and what they are planning to do in the near future.

- Chapter IV— Assessment of Risks, shows the ability of companies to assess their security risks, and the measures they are taking to address them.

- Chapter V— Satisfaction with Security Products and Services, identifies how effectively electronic commerce security products are meeting users' needs.

- Chapter VI — Security Purchasing, identifies the key characteristics involved in selecting vendors for electronic commerce security products.

D
Related INPUT Reports and Research Bulletins

Evaluation of Firewall Solutions, U.S., 1997

Evaluation of Internet Firewall Solutions, Europe

Evaluation of Internet Firewall Solutions, France

Enabling Storefront Security, 1997

One-Time Passwords Address a Growing Problem, Research Bulletin, 1997

II

Executive Summary

A
Overview

The electronic commerce security industry is undergoing tremendous evolution, with many vendors consolidating, merging, and forming alliances. However, many clients are having difficulty developing electronic commerce capabilities. Products remain difficult to use, solutions do not fully meet their expectations, and knowledgeable staff is difficult to find. To avoid these problems, vendors should:

- Make products easier to use and manage by providing multi-platform and multi-vendor support across the enterprise.
- Reduce risk by ensuring that 128-bit encryption is available internationally.
- Provide more first-hand product exposure and hands-on training through seminars and tradeshows.

B

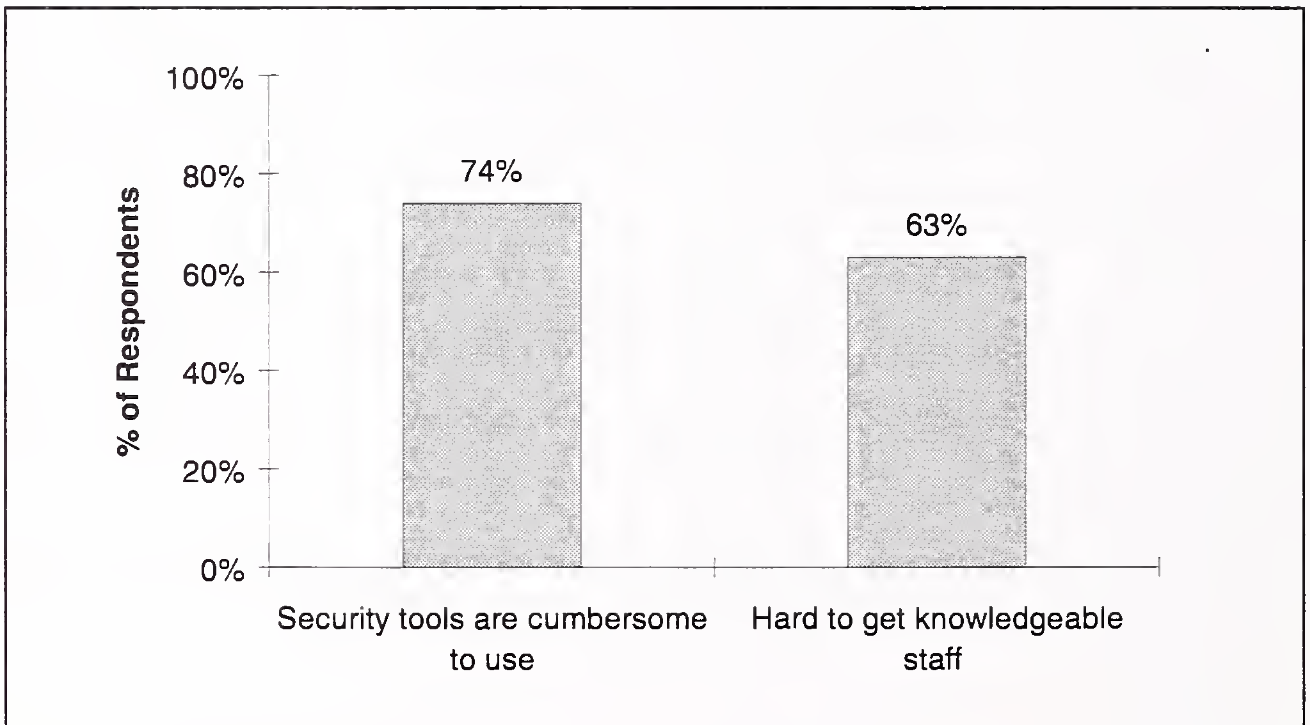
Make Products Easier to Use

Highly trained and competent personnel are required to set firewall rules, monitor security newsgroups, apply software patches, audit system logs and utilize real-time intrusion detection software. In a large enterprise environment, such personnel often must be expert in the use of dozens of applications running on a variety of different platforms and environments. The failure to regularly perform these functions competently can result in significant security problems.

As Exhibit II-1 shows, users find existing tools to be complex and difficult to learn and use, making it difficult to identify, attract, train, and retain staff knowledgeable in their use.

Exhibit II-1

Problems with Security Products



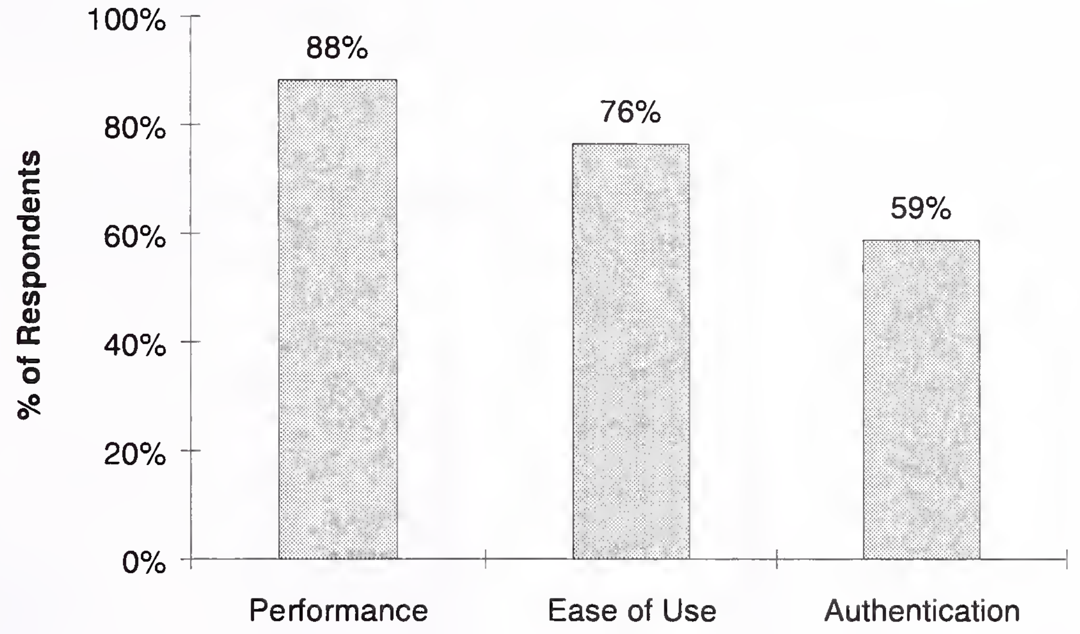
Number of Respondents: 46

Source: INPUT

Looking at this issue slightly differently, Exhibit II-2 shows how important authentication, ease of use, and performance are to users.

Exhibit II-2

Respondents Rating Feature as "Most Important"



Number of Respondents: 51 *Source: INPUT*

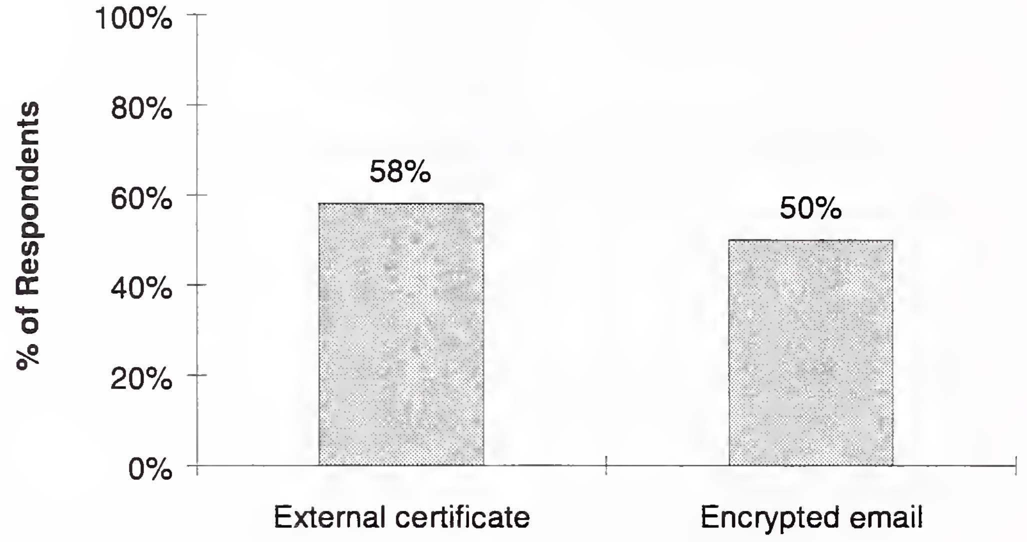
Numerous vendors are beginning to offer security packages with enterprise level functionality, supporting a wide range of clients, data transports, servers and operating systems. While these packages often improve security personnel effectiveness, considerable room remains for improvement in ease of use and performance.

C
Reduce Risk

One of the most common methods of reducing risk is through the use of encryption technology. As Exhibit II-3 illustrates, a wide deployment of encrypted email and certificate servers supporting encryption keys is occurring, indicating the seriousness of efforts being taken to reduce the risk of data being compromised.

Exhibit II-3

Current Deployment of Encryption Technology



Number of Respondents: 52 *Source: INPUT*

Using specially designed hardware, it is possible to decrypt messages generated by 40-bit and 56-bit keys. Consequently, many users correctly believe that such encryption can no longer be regarded as completely secure.

Two examples of vendors addressing this issue are Germany-based Brokat Information Systems and United States based C2Net. Brokat downloads a Java applet allowing 128-bit encryption to be performed, even though the user's browser may normally only support 40-bit encryption. C2Net provides a secure version of the popular Apache web server using 128-bit and longer keys. By developing its cryptography products outside of the United States and backing them with U.S.-based sales and marketing, C2Net is able to offer secure cryptography products worldwide. Vendors should make every effort to use the latest 128-bit encryption technology to ensure the integrity of their products.

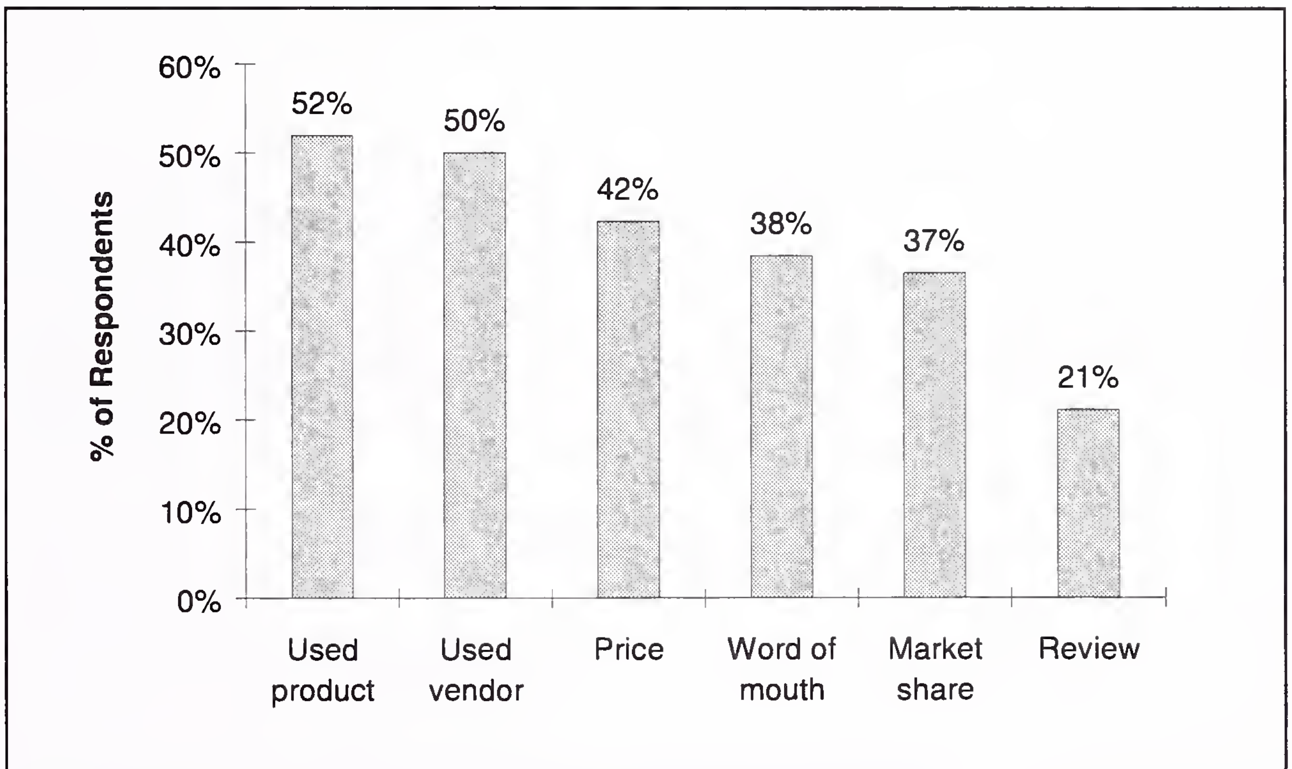
D

Provide More First-Hand Product Exposure

There is a need for vendors to provide more first-hand product information to existing and potential customers. The benefit of providing more first-hand product experience is demonstrated in Exhibit II-4. Respondents cited which sources of information were most important in influencing their electronic commerce security buying decision.

Exhibit II-4

Influences on Buying Decision



Number of Respondents: 51

Source: INPUT

The low impact of media product reviews indicates seminars and other methods of achieving face-to-face contact with the customer will have superior value to print media in establishing credibility and awareness.

III

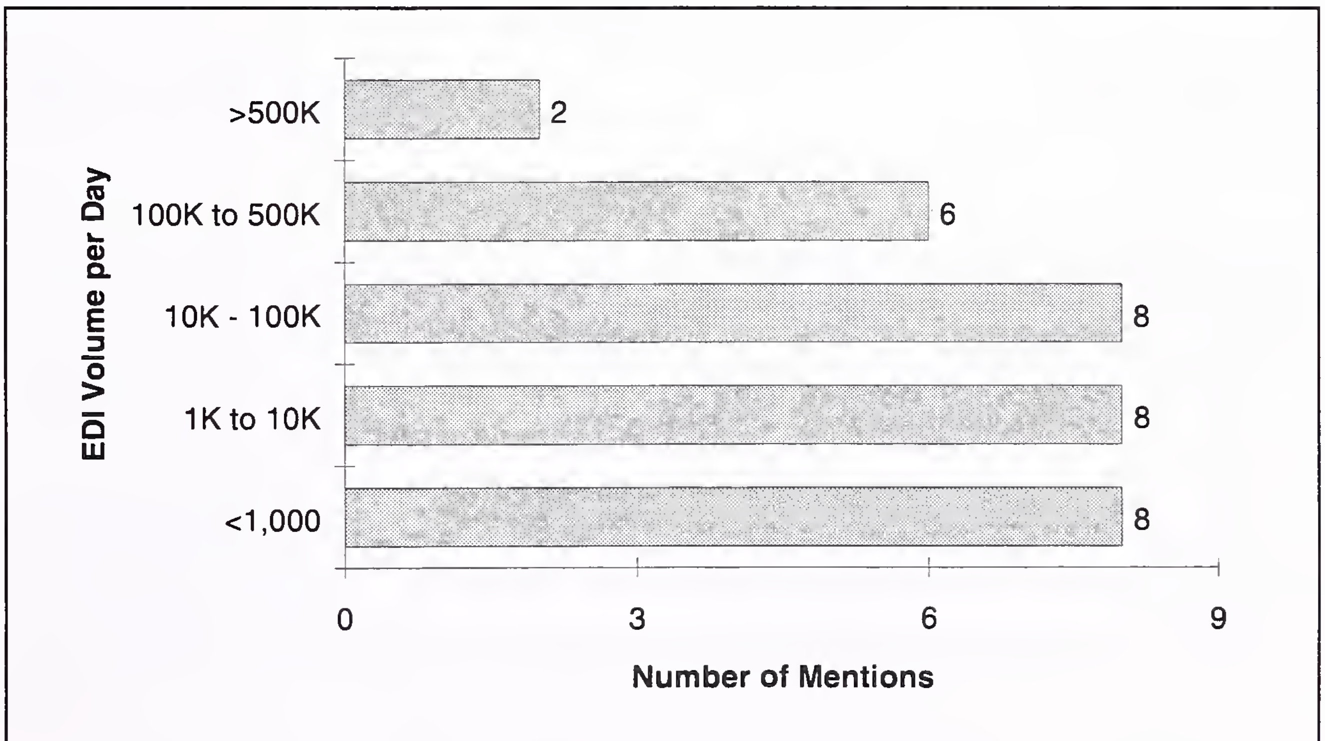
Usage of Electronic Commerce Security Products and Services

A
Current and Planned Usage of Electronic Commerce

This chapter examines how buyers are using electronic commerce security products and their short-term plans. Exhibit III-1 shows the number of transactions that occurred over the respondents' systems.

Exhibit III-1

EDI Transaction Volume per Day



Number of Respondents: 32

Source: INPUT

Electronic commerce has both reduced the entry cost as well as increased the growth of EDI, especially for performing business to business transactions. As Exhibit III-1 indicates, 64% of the respondents were able to state a precise daily volume of transactions. The vast majority of these transactions were by EDI or other internal transaction networks. The average number of transactions per day was 185 thousand. A finance and healthcare company accounted for the two highest volumes at four million and 500,000 transactions per day, followed by several manufacturing companies.

Traditionally, EDI has been provided by companies such as General Electric Information Services (GEIS), IBM Global Information Network (Advantis), Sterling Commerce, Inc. and Harbinger Corp. Recent arrivals such as Internet Commerce Corporation, Netscape Communications, OpenMarket, Pandesic, and The EC Company are attempting to enter the EDI market.

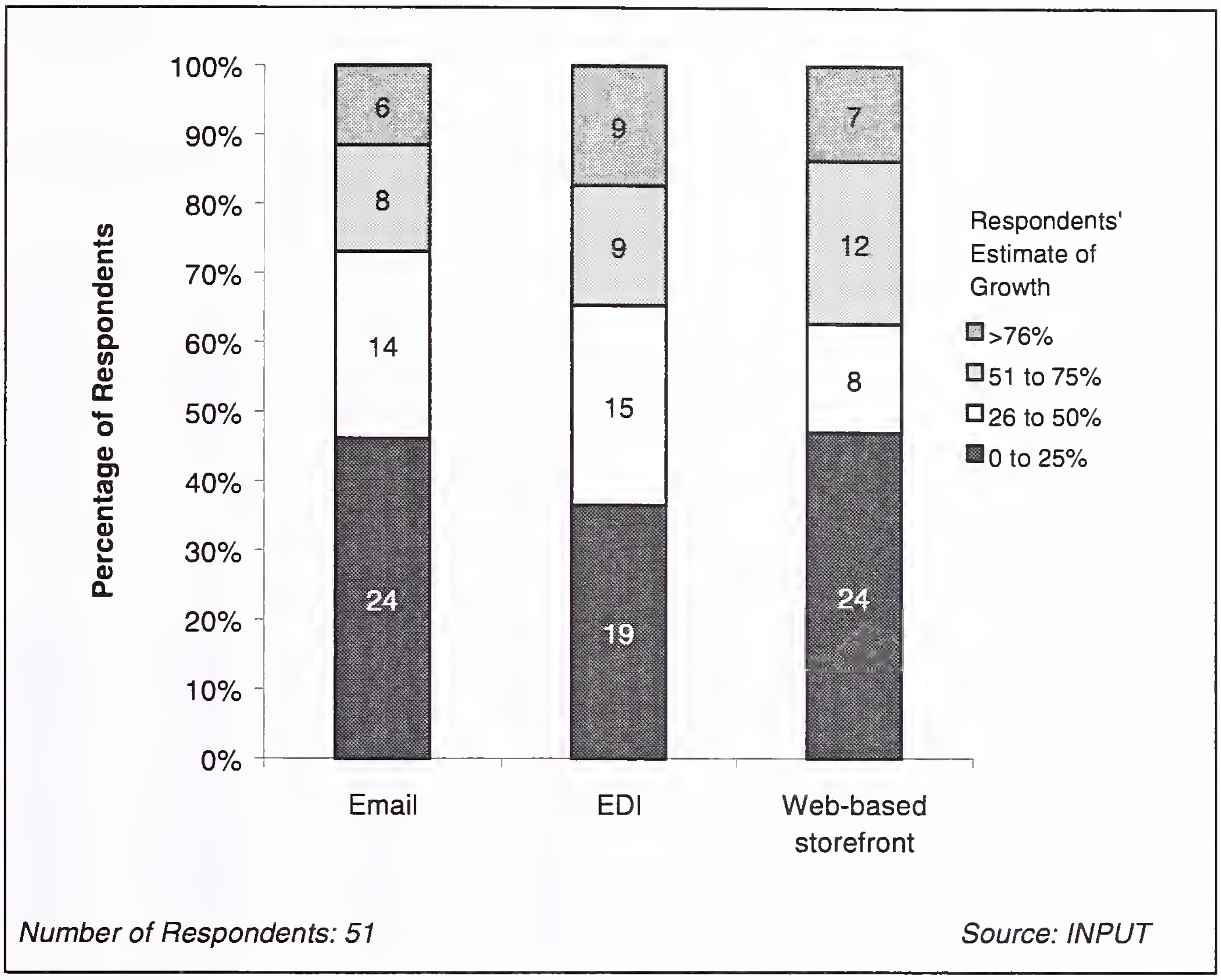
Respondents were asked the rate of growth they saw in the following areas:

- Email
- EDI
- Web-based storefront.

Exhibit III-2 shows the results of this question:

Exhibit III-2

Growth of Applications



Number of Respondents: 51

Source: INPUT

Overall, respondents saw EDI as growing slightly faster than Web-based stores and Email. This result is somewhat biased due to the heavy EDI use of many of the respondents. But the majority of respondents saw all three areas as having growth rates exceeding 25% over the next year.

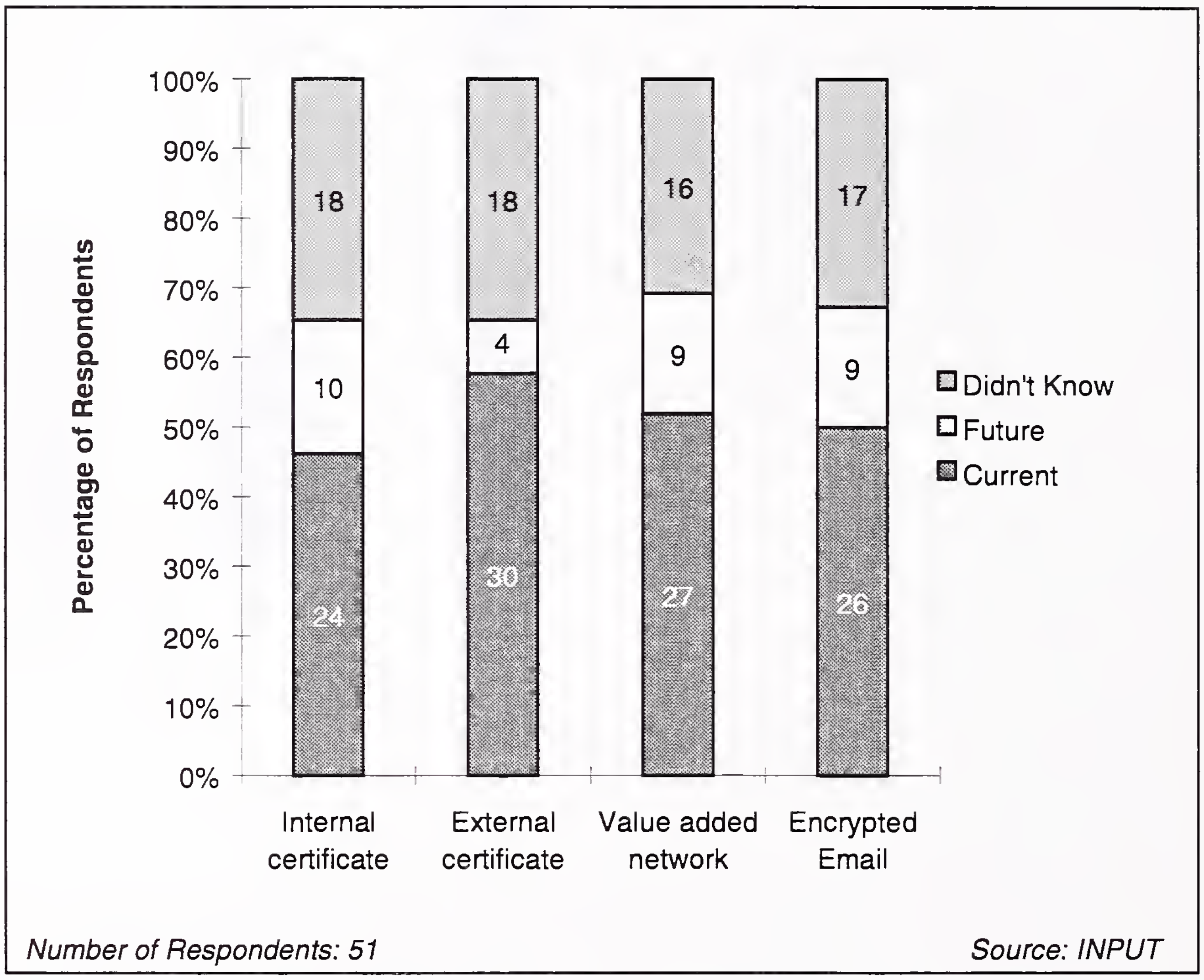
From a security standpoint, existing email has problems with a lack of confidentiality, authenticity, integrity and non-repudiation. The use of secure email will become common as the integration and standardization of encryption, digital signature, and integrity services improve its ease of use.

B
Current and Planned Usage of Security Products and Services

Exhibit III-3 shows the results of respondents being asked what electronic commerce security services they used or planned to use in the future.

Exhibit III-3

Current and Future Use of Security Services



Number of Respondents: 51

Source: INPUT

Over 60% of the respondents stated that they were currently using either internal or external certificate servers. Given the relatively low volume of certificate activity from the industry leaders such as Verisign, it is apparent that certificate use is not yet widely deployed. Since many of the respondent companies are of substantial size, this suggests that use of certificate servers can be expected to rapidly increase. As would be expected from the high EDI transaction volumes, 54% indicated that they were making use of value added networks.

A standard for encrypted and digitally signed email is S/MIME. Developed by RSA (now part of Security Dynamics), this standard allows sending encrypted email and verifying the authentication of received messages. Secure email systems typically use public key encryption with certificates to verify the authentication of each message. A notable exception to using certificates is the PGP (Pretty Good Privacy) implementation, now owned by Network Associates. In this scenario each user maintains a list of the public keys for the recipients of their email messages.

In many cases users are sending secure email without being aware of it, due to the efforts of the system administrator. For example, approximately 20 million Lotus Notes are sent in encrypted form each day by seven million users.

There are many companies providing secure email and/or certificate services. Verisign is an RSA spin-off company providing public certificate services. IBM and Equifax are jointly promoting and offering public certificate servers; IBM through its IBM Vault Registry service and Equifax by providing outsourced digital certificate services to IBM customers. AT&T Secure Communication provides its SecretAgent product, a digital signature and encryption utility that uses public key certificates and is only available on Windows. Nortel Secure Networks Entrust was one of the first commercial products to provide certificate authorities, key management and public key infrastructure. Additionally, Netscape builds knowledge of certificate servers into its web server and browser products.

While Value Added Networks (VANs) have traditionally been provided by third party vendors over proprietary networks, a large number of vendors are offering the capability of forming private VANs over public networks by using a combination of firewalls and transparent encryption to form secure "tunnels" across the Internet. Israel-based CheckPoint Software, the market leader of firewall products with a 45% market share, provides such a module, as does Sun Microsystems.

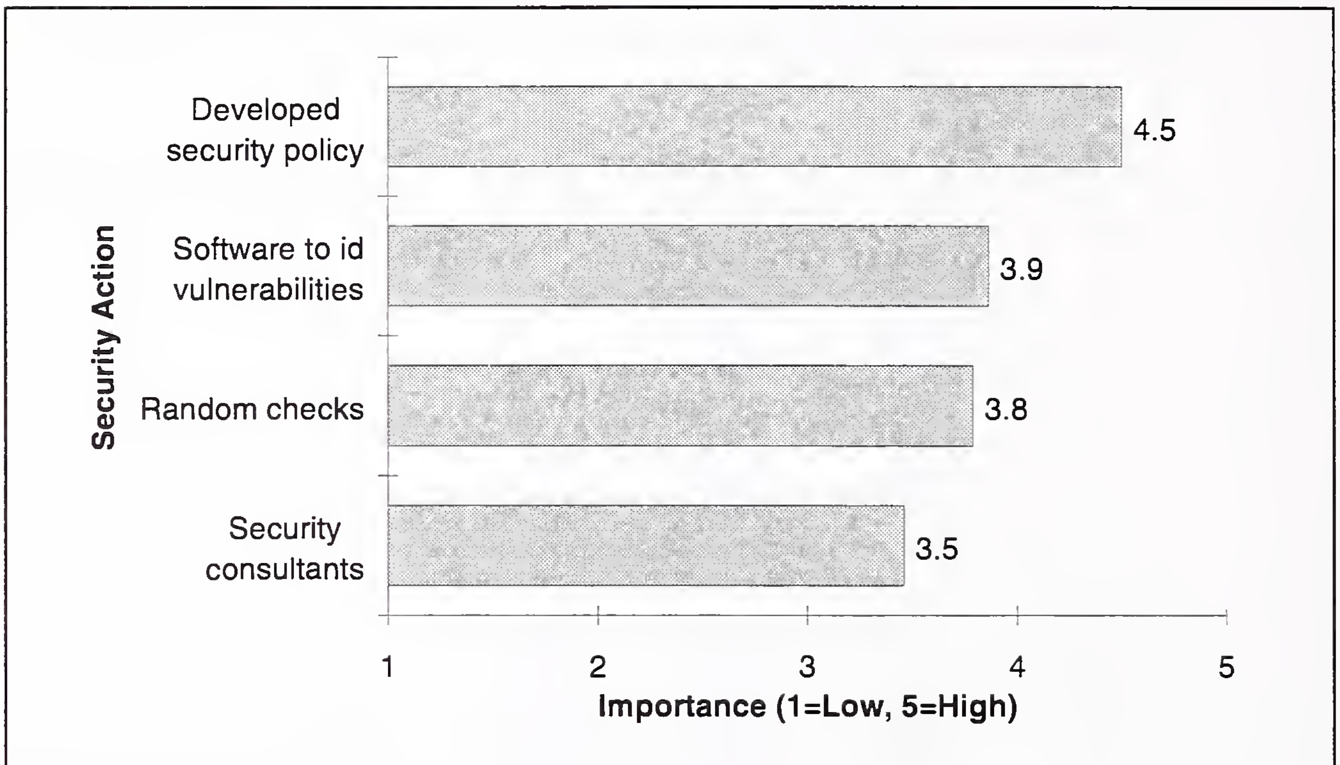
Respondents were asked to rate the value of the following for helping to minimize their electronic commerce security risks:

- Security policy developed in-house
- Security consultants
- Use software to systematically identify vulnerabilities
- Periodically do random checks to test security procedures.

Exhibit III-4 shows the results of this question:

Exhibit III-4

Importance of Actions for Reducing Security Risks



Number of Respondents: 51

Source: INPUT

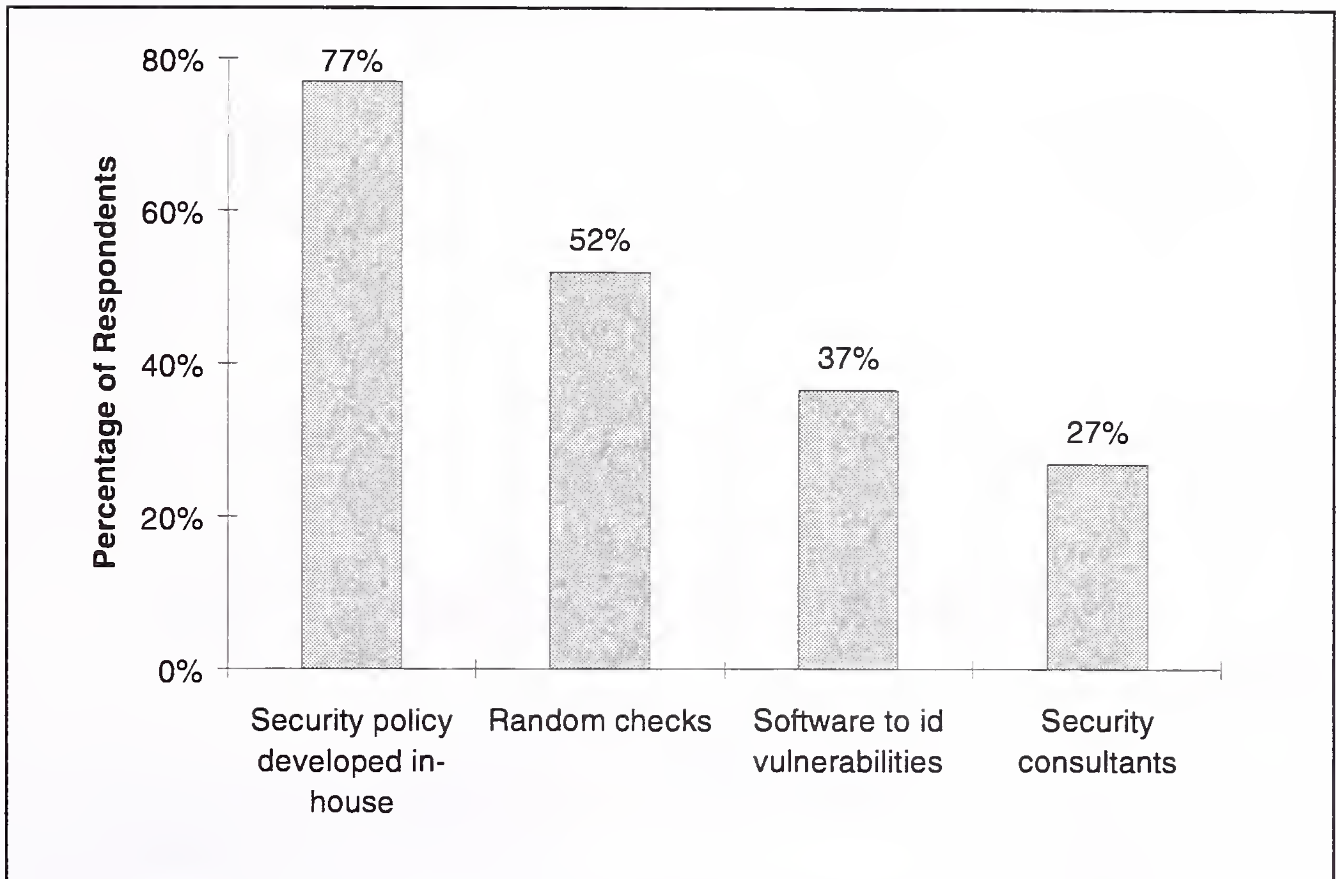
There are many software packages that help to identify and verify proper network security and vulnerabilities. Examples include Bellcore's PINGWARE, Infostructure's NetProbe, and ISS's Internet Security Scanner and SATAN. For vendors attempting to provide a total electronic commerce security package, these results suggest that they should strongly consider providing a module to systematically probe and identify security vulnerabilities.

Consistency is the key to effective security. Many organizations lack the resources or expertise to effectively monitor their critical systems. Having a security consultant regularly run security programs that identify potential problems can be a cost-effective solution for many companies.

Exhibit III-5 shows the results of asking respondents which security activities were actually being practiced.

Exhibit III-5

Actions Actually Being Performed



Number of Respondents: 51 *Source: INPUT*

While most respondents had implemented a security policy, only 37% had acquired software for systematically identifying vulnerabilities, despite its being seen as being more effective than random checks. This suggests there is room for this market to grow substantially.

In keeping with the view that security consultants were the least effective way of reducing security risks, only 27% of the respondents reported using them. This is ironic, since using a consultant to conduct an actual intrusion test where attempts are made to actively penetrate a site is one of the most effective ways of verifying a firewall system. But at the same time, it is understandable that many organizations are unwilling to undergo this "experience," since penetration testing can disrupt operations and destroy data unless proper precautions are taken.

There are many companies providing security software services. Two examples are MIS Europe, which provides a range of security consulting services, and the SGS Group who provides security auditors that verify that an organization's security methods and procedures are being followed.

In Exhibits III-6, III-7, III-8 and III-9, respondents were asked whether or not they were using or planned to use a specific type of electronic commerce security product.

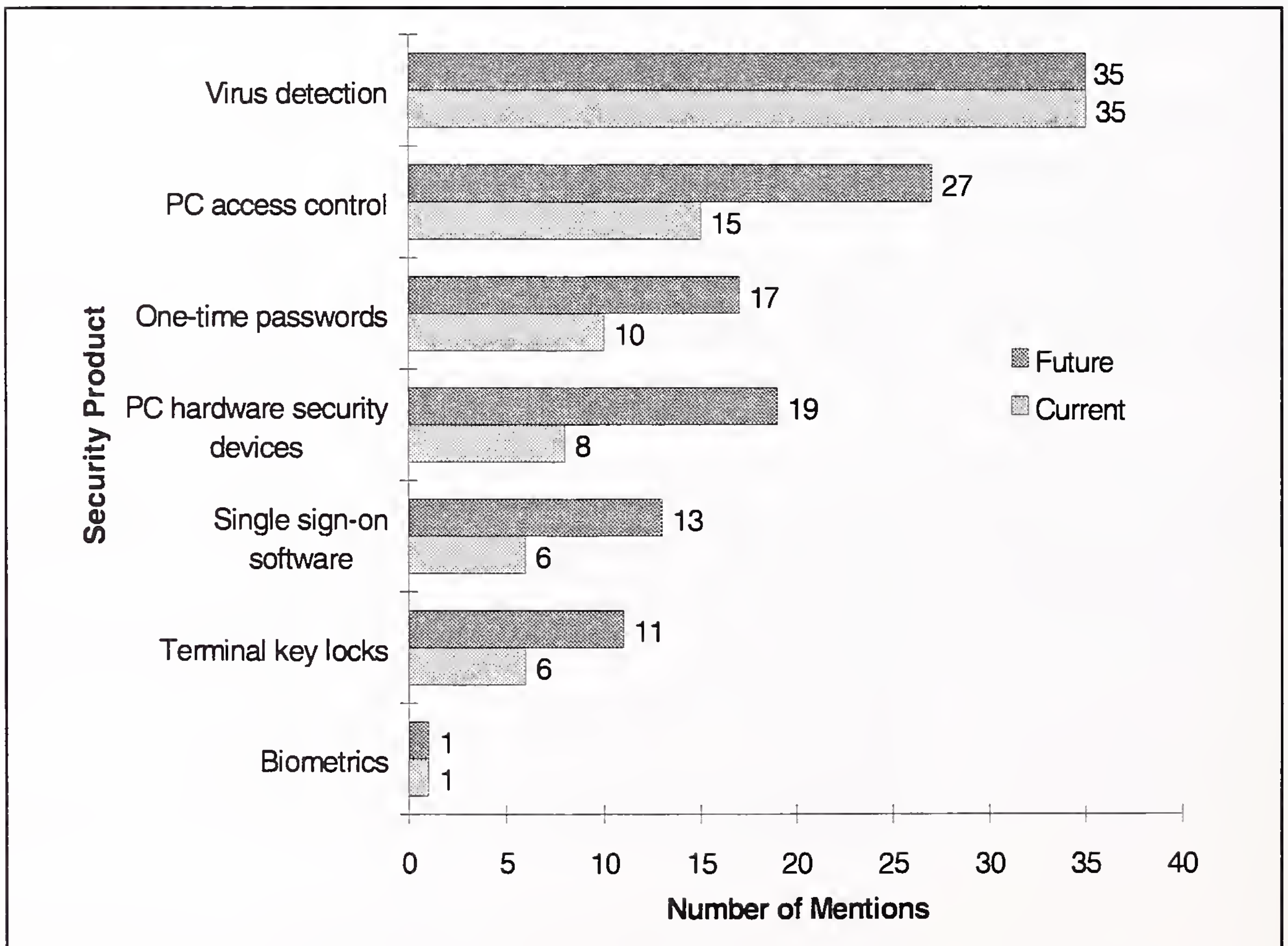
For the purpose of making this analysis easier to comprehend, we have divided a diverse set of electronic commerce security products into four categories:

- Client
- Data Transport
- Server
- Operating System.

Obviously, attention must be addressed to each of these areas in order to provide effective electronic commerce security.

Exhibit III-6

Current and Future Use of Client Security Products



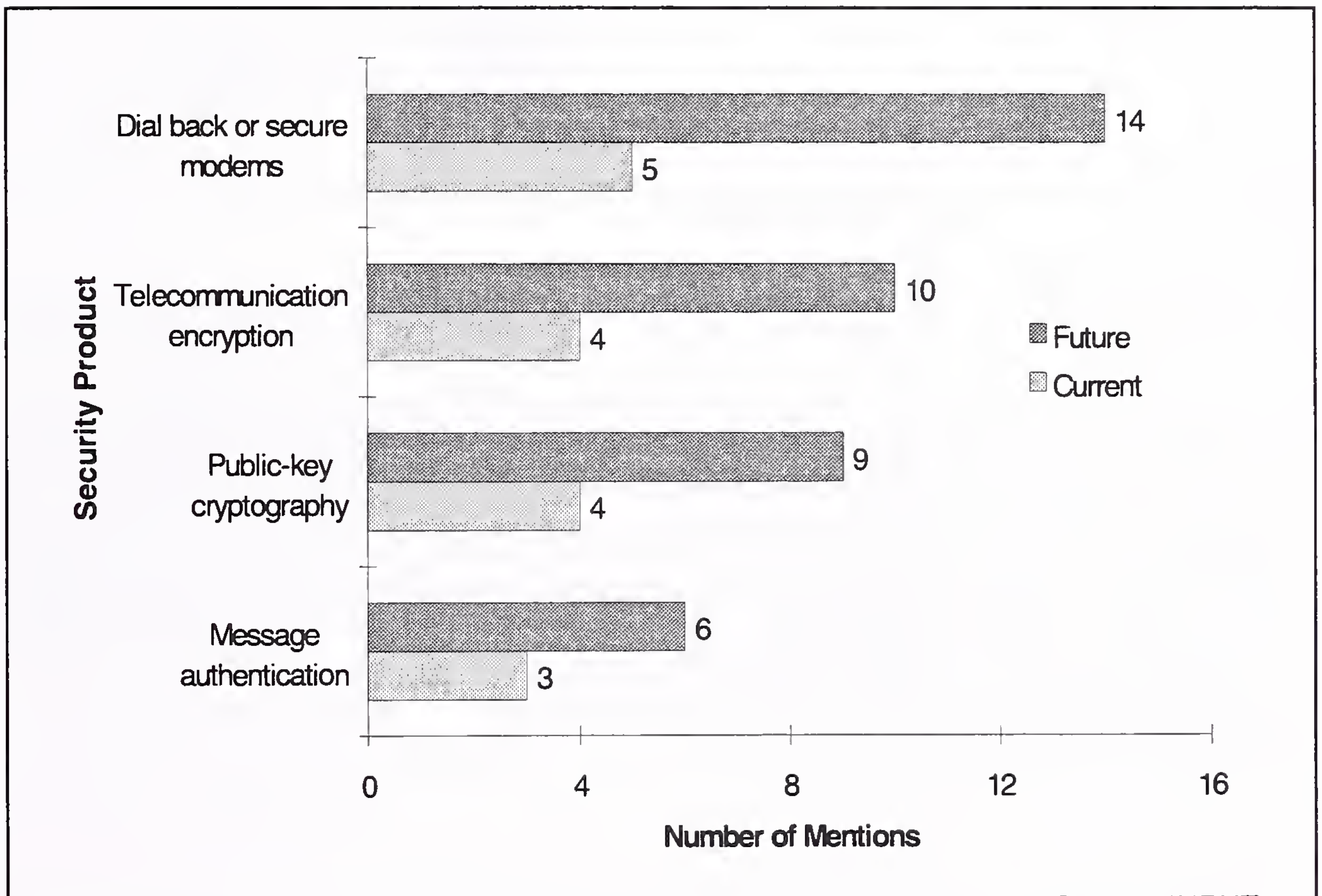
Number of Respondents: 35 *Source: INPUT*

As shown in Exhibit III-6, virus detection and eradication are the single most common problem being addressed on client products. A variety of client access controls and authentication techniques are being examined or considered, but biometrics technology such as voice recognition, handwriting analysis, and iris detection are not considered viable technologies by the respondents.

Many companies are trying to make client security products more integrated, since intrusive security mechanisms tend to stimulate users to find ways of circumventing them. For example, many enterprise security programs provide a single logon and password for a user to access multiple systems.

Exhibit III-7

Current and Future Use of Data Transport Security Products

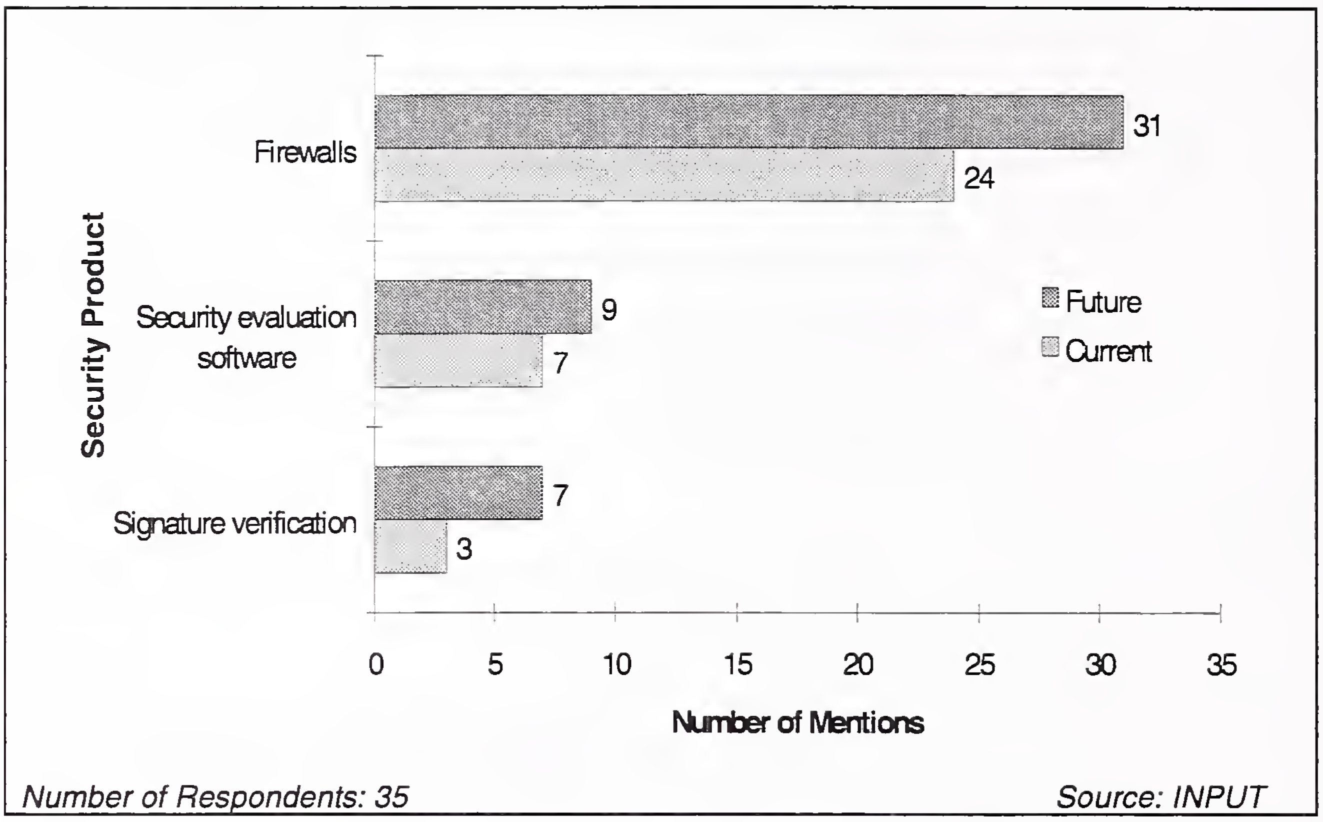


Number of Respondents: 35 *Source: INPUT*

A tremendous amount of media attention has been placed on data transport protocols such as SSL (secure socket layer) and electronic cash protocols by vendors such as DigiCash, CyberCoin, Mondex, CAFE and Visa Cash. But the survey results indicate that respondents are more focused on traditional methods of providing data transport security such as dial-back modems.

Exhibit III-8

Current and Future Use of Server Security Products



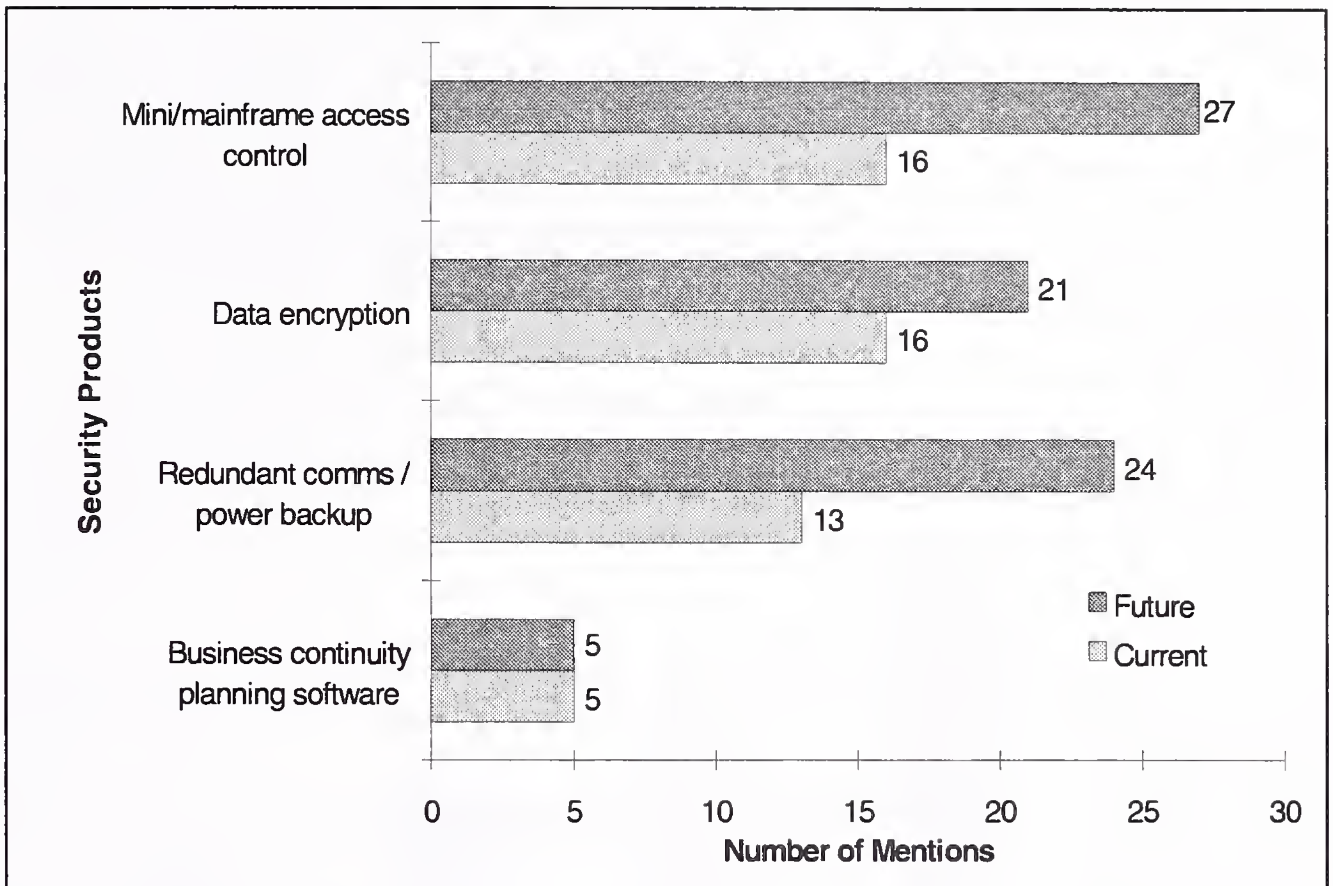
Number of Respondents: 35

Source: INPUT

Firewalls are the most common and popular way of insuring server security. In the survey, Checkpoint Software's Firewall-1 was the most commonly mentioned product, consistent with its large market share. Approximately one-third of firewall respondents indicated that they were also using security evaluation software. The small number planning to use such software in the future, relative to the number of firewall users, suggests that vendors of such software need to engage in a campaign to both educate and build awareness of the advantages and value of using such software on a continual basis.

Exhibit III-9

Current and Future use of Operating System Security Products



Number of Respondents: 35 *Source: INPUT*

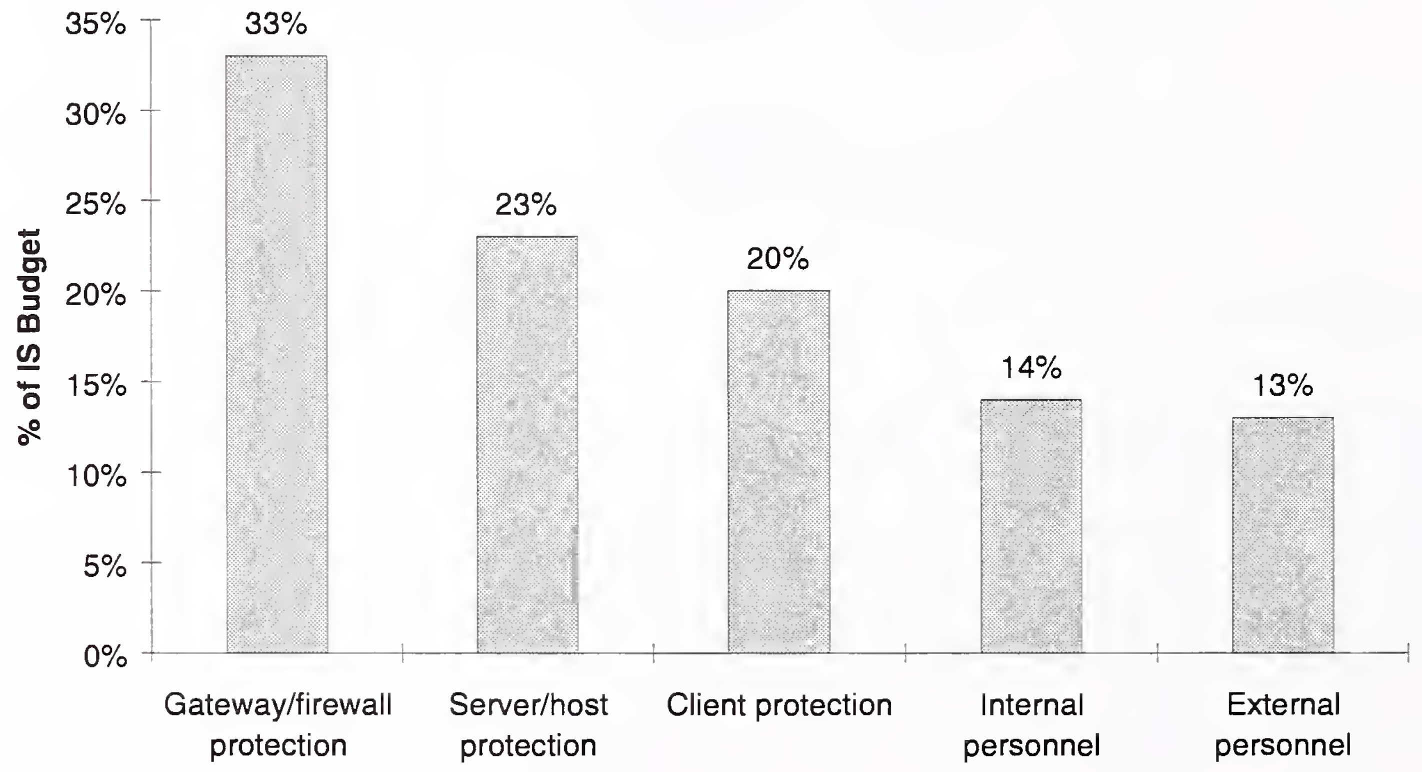
The number of respondents indicating the use, or planned use of access control, data encryption and power backup equipment, indicates that the operating system and its hardware are being regarded as critical business resources. Yet comparably little use is being made of business continuity planning software to help systematically develop contingency plans. At the same time, the lack of deployment of many of the above measures suggests that while the majority of respondents have developed security policies, these policies may not have completely assessed the value of company information.

C
Security Related Expenditures

The survey sought to understand what portion of the IS budget was devoted to security, and how this security budget was allocated to client protection, gateway/firewall protection, server/host protection, and internal and external personnel. Exhibit III-10 shows the average security budget allocated to these functions.

Exhibit III-10

Allocation of Security Budget



Number of Respondents: 25

Source: INPUT

Forty years ago, labor costs accounted for practically the entire security budget. By 1998 labor accounted for only 25% of expenditures. However, significant time and resources are still required by security personnel to effectively protect corporate information systems. For example, security personnel are required for issuing passwords, setting firewall rules, monitoring security newsgroups, applying software patches, auditing system logs and utilizing real-time intrusion detection software. Human error and the “if it isn’t broke, don’t fix it” syndrome remain significant issues, because even when problems are identified and patches are implemented, they often are not installed correctly, leaving systems vulnerable to attack.

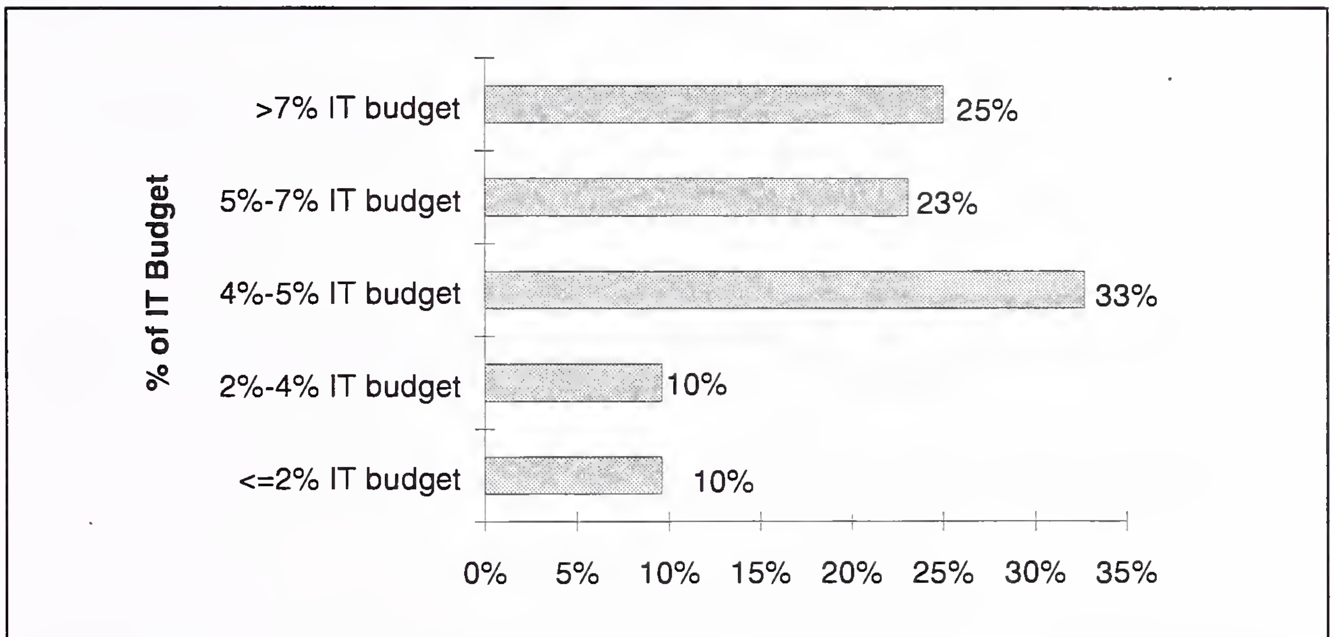
To help improve productivity and the consistency of administering electronic commerce security, many software vendors are providing packages with enterprise level functionality, which support a wide range of clients, data transports, servers and operating systems.

In line with the widespread use and deployment of firewalls, they account for almost one-third of the overall security budget. Over the next few years firewalls will become easier to manage, decrease in cost, and provide transparent encryption with firewalls from other vendors. In this context, firewall products can eventually be expected to become commodities.

Exhibit III-11 provides a chart showing the variation in the proportion of the IT budget that respondents devote to security.

Exhibit III-11

Portion of IT Budget Devoted to Security



Number of Respondents: 49

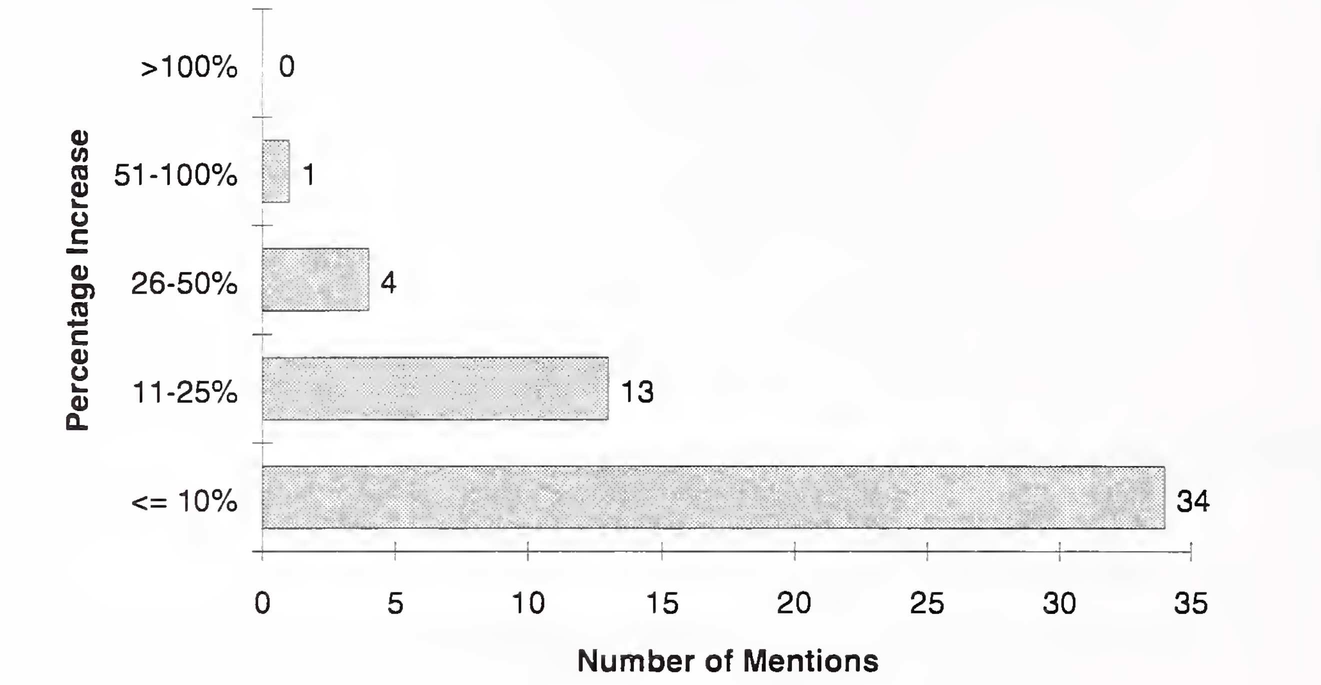
Source: INPUT

On average, 6% of the IT budget is being devoted to security. For vendors, growth will continue to be strong, both from expansion of current accounts, as well as new users deploying their initial implementations. The trend will continue towards spending less of the security budget on personnel and more on software for improving security personnel effectiveness.

Exhibit III-12 shows the respondents' expected increase in IT security budgets.

Exhibit III-12

Percentage IT Security Budget Will Be Increased



Number of Respondents: 52

Source: INPUT

Over a third of the respondents indicated their IT security budget would be increased by over 10% in the following year.

IV

Assessment of Risks

A Importance and Difficulty of Preventing Security Violations

Dan Farmer, the author of SATAN, a well-known tool for identifying system vulnerabilities, noted that “security on a computer system degrades the more you use the system." The more a product is used and examined, the more flaws, deficiencies, and vulnerabilities that will be found. Since most electronic commerce products will continue to experience increased growth over the years to come, security will remain a central issue.

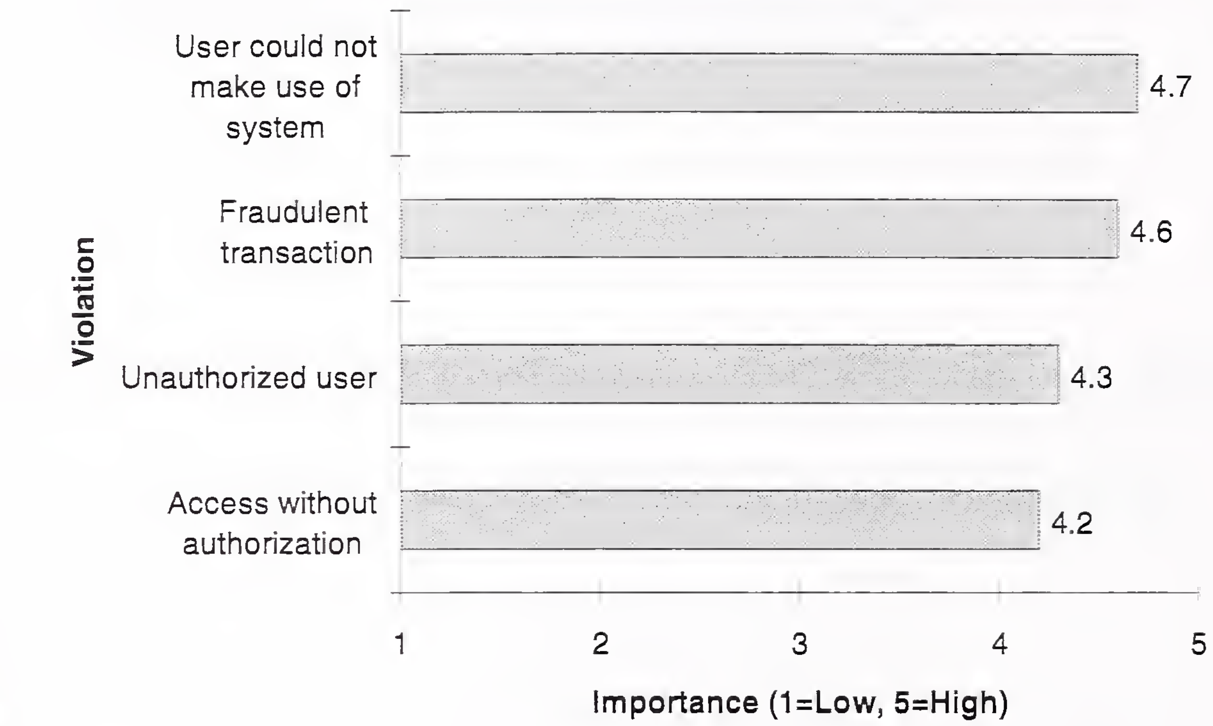
The survey measured how respondents viewed the importance and difficulty of preventing the following security violations:

- Users could not make use of system due to the security violation
- Databases / web accessed without authorization
- Fraudulent transaction
- Unauthorized user.

Exhibit IV-1 compares the different responses for the importance of preventing security violations.

Exhibit IV-1

Importance of Preventing Security Violations



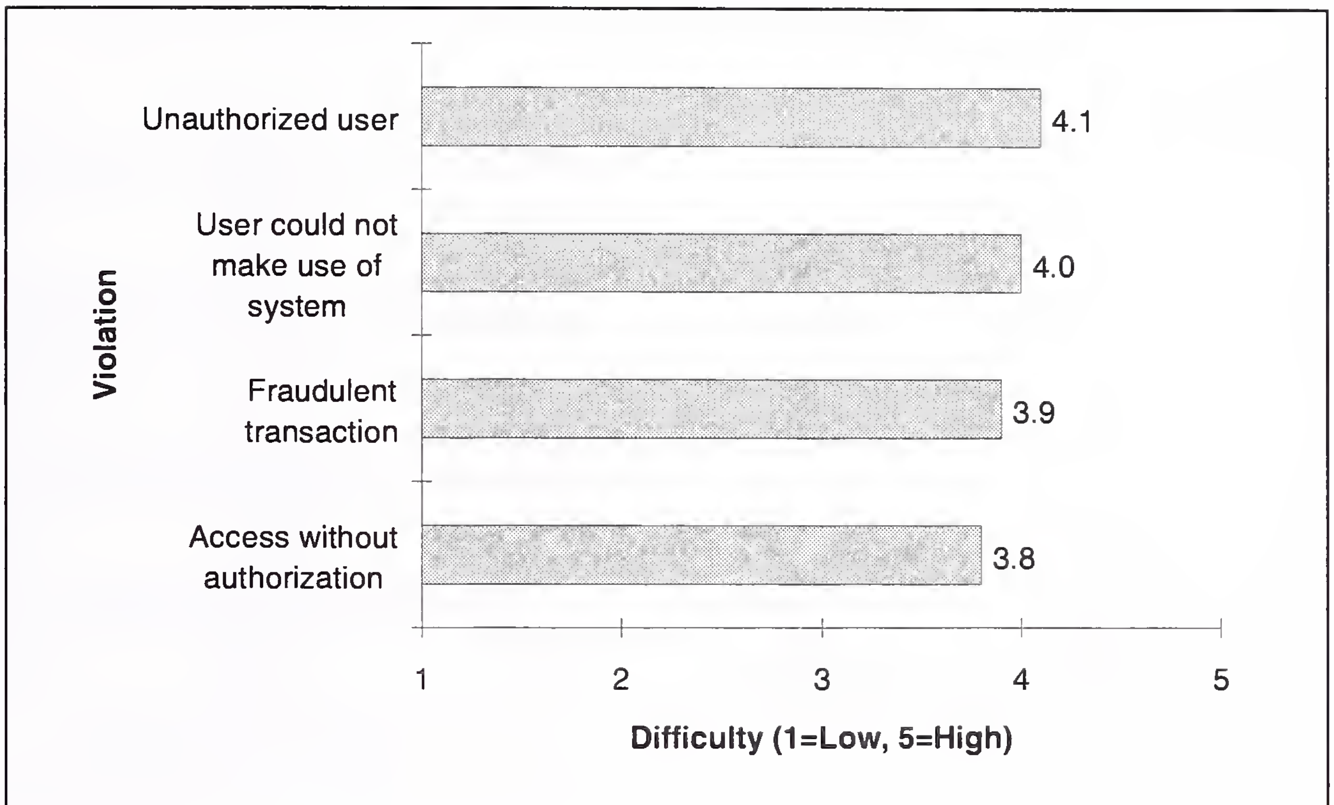
Number of Respondents: 51 *Source: INPUT*

Insuring system availability was seen as having the highest importance, much in keeping with the critical business nature of the systems being used. The implied value of high availability suggests that supporting and promoting fault-tolerant features would be a strategic move by vendors promoting enterprise-wide security solutions.

Exhibit IV-2 compares the different responses concerning the difficulty of preventing security violations.

Exhibit IV-2

Difficulty of Preventing Security Violations



Number of Respondents: 51 *Source: INPUT*

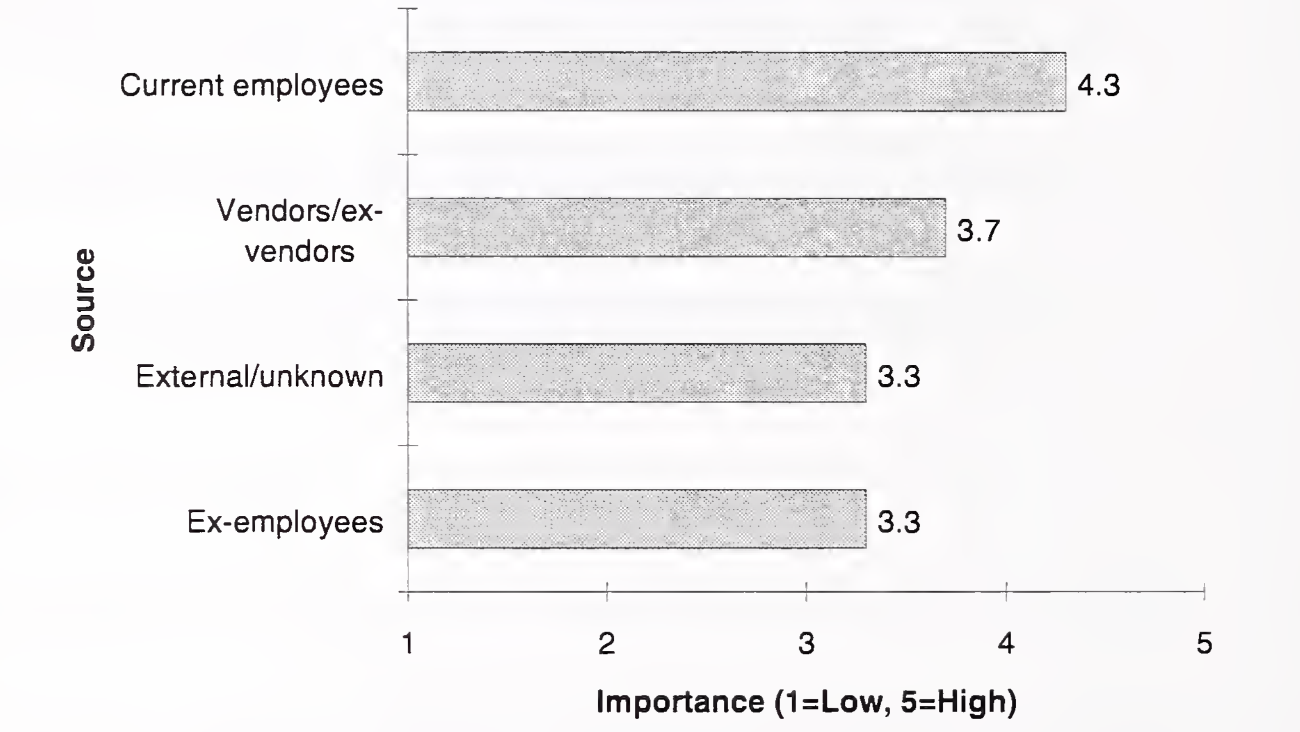
Respondents regard each of the four areas to be equally difficult in preventing a security violation. Many security experts regard insuring proper authorisation as a very difficult problem. For example, users often write passwords down on Post-It Notes. Improved authentication can be provided by solutions such as user certificates on smart cards. This type of measure will avoid problems caused by existing password-based authentication methods.

B
Sources of Security Violations

The survey sought to provide insight into the sources of security violations. Exhibit IV-3 shows the relative importance that respondents assigned to different types of security penetration.

Exhibit IV-3

Importance of Security Penetrations



Number of Respondents: 23

Source: INPUT

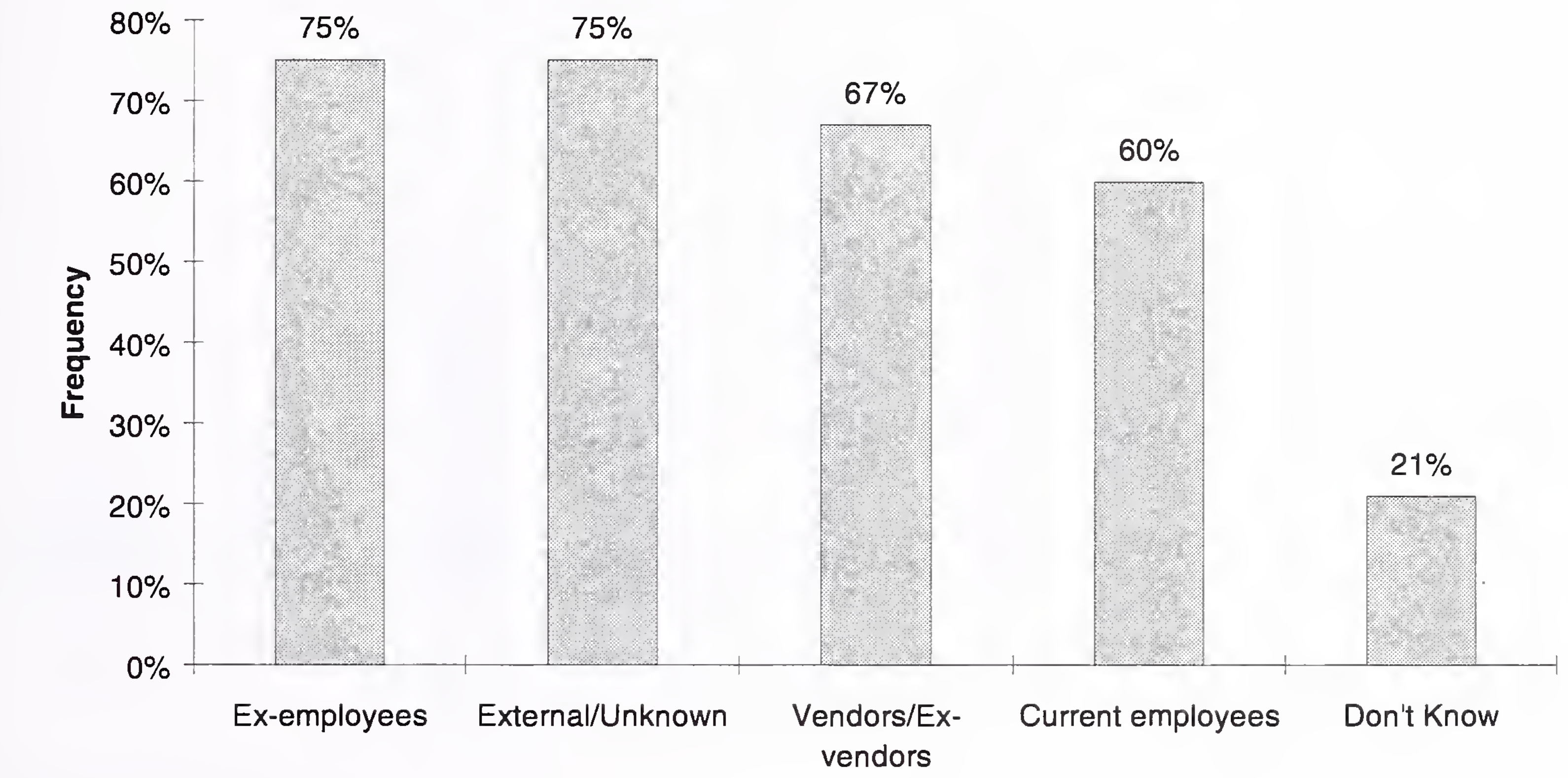
Interviews with security violators suggest that employees are motivated by financial gain and revenge. External threats are typically motivated by factors including idealism, curiosity, need for recognition, a desire to create disruption, and espionage.

Given the results of the survey, primary attention should be addressed in insuring that employees and vendors are restricted in the types of information they can access. This is not to say that former employees and external threats should not be considered, only that the respondents considered them to be somewhat less likely to occur.

Exhibit IV-4 shows the weighted-average relative frequency for different categories of security violations.

Exhibit IV-4

Actual Sources of Security Penetration



Number of Respondents: 23

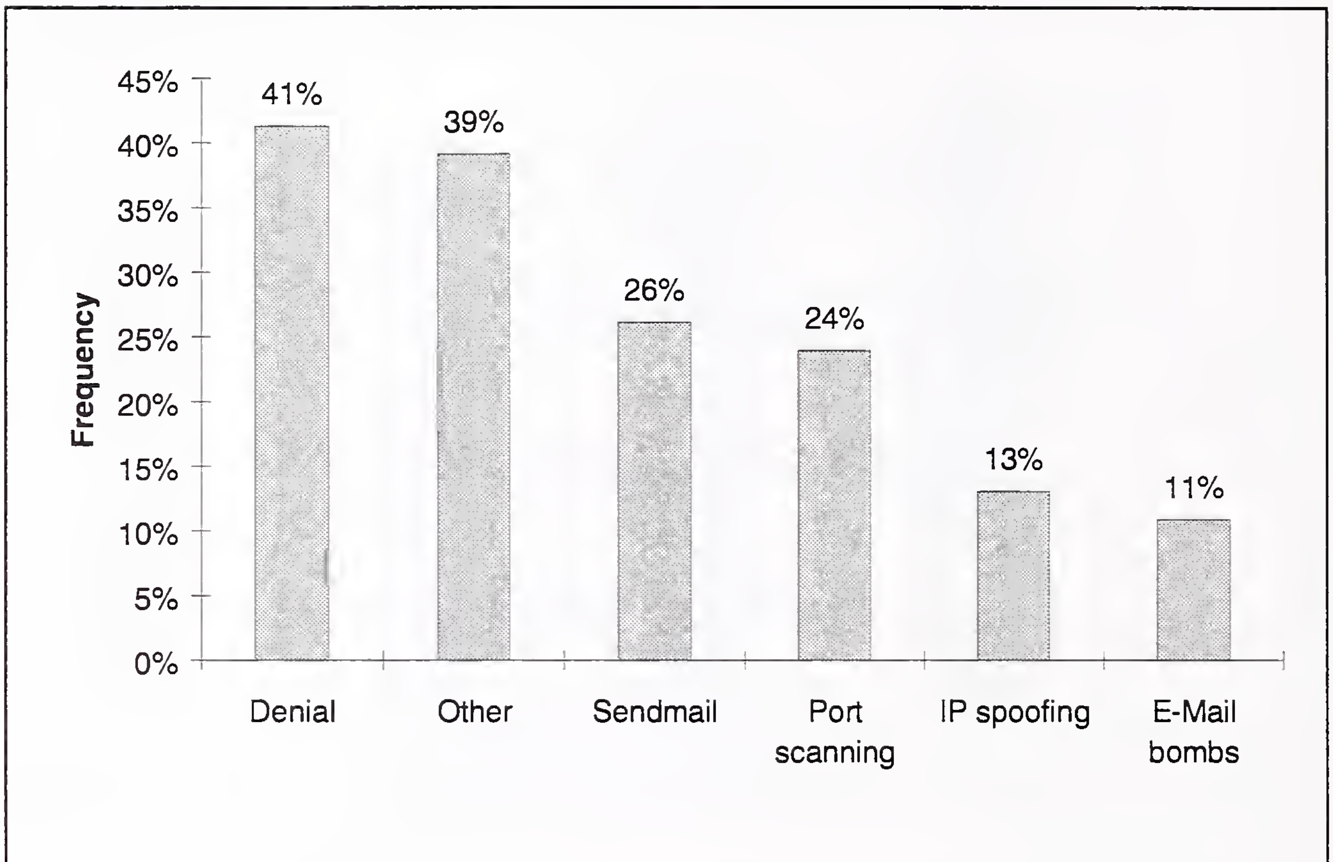
Source: INPUT

What is interesting about this exhibit is that it is almost the reverse of Exhibit IV-3 in that external and ex-employees were most frequently cited as being the source of a security violation. It is perhaps only human to think of security threats as being external, when in fact the most frequent, serious, and difficult to prevent attacks often come from within the organization.

Exhibit IV-5 illustrates the different types of attack that have been experienced by the respondents.

Exhibit IV-5

Types of Attack Experienced



Number of Respondents: 46 *Source: INPUT*

The types of attacks cited here are Internet-specific, with the exception of viruses, the most frequently mentioned "other" type of attack. Denial of service attacks is very difficult to defend against due to the nature of the TCP/IP protocol. In these attacks, a site will be flooded with hundreds of incomplete Internet connections per second, preventing valid requestors from accessing the site.

Sendmail (SMTP) is the most commonly used email system on the Internet since it is available on most versions of Unix. Due to its complex nature, many bugs and back doors have been found in it, making it difficult to prevent security violations. Many sites run other mail programs such as Lotus Notes or cc:Mail internally to eliminate this vulnerability.

Port scanning occurs when software such as SATAN is used to systematically identify the IP ports on a system. Ideally, a firewall performing packet filtering should be used to block various ports and drop certain IP packets. In essence, port scanning is analogous to a thief examining a car in order to see which doors are open and whether or not the keys are in the ignition.

IP spoofing is when an attacker uses a pseudo host name in an attempt to fool a server about their true identify. Typically this can be detected when the host name and IP address do not agree with DNS (domain name service) tables. In Web spoofing, users may be conned into using a "shadow" copy of a site, and inadvertently disclose private information, or be given false or misleading information.

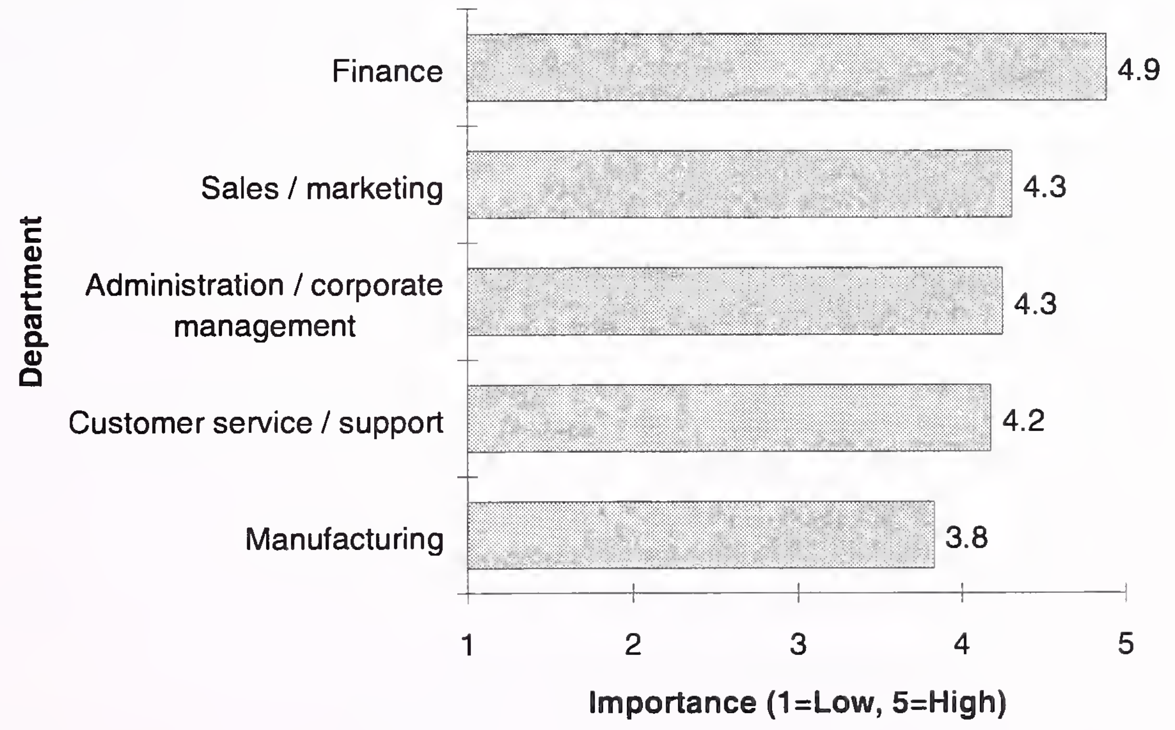
E-mail bombs are a particular Sendmail attack in which mail is redirected to a file instead of an individual, and Sendmail is caused to compile and execute that file as a program, where it creates a backdoor into the system. While these attacks are very sophisticated and do not occur frequently, a significant number of sites have experienced them.

C
Importance of Security by Department

Exhibit IV-6 shows the importance of security in electronic commerce with respect to different departments.

Exhibit IV-6

Importance of Security by Department



Number of Respondents: 51

Source: INPUT

There was essentially universal agreement that the finance department contained the most vital information that needed to be secured. Many of the service companies had essentially no manufacturing function, accounting for its lower average ratings. Manufacturing-centric companies gave equal importance to their manufacturing data as they did their financial data.

V

Satisfaction with Security Products and Services

A Problems with Security Products

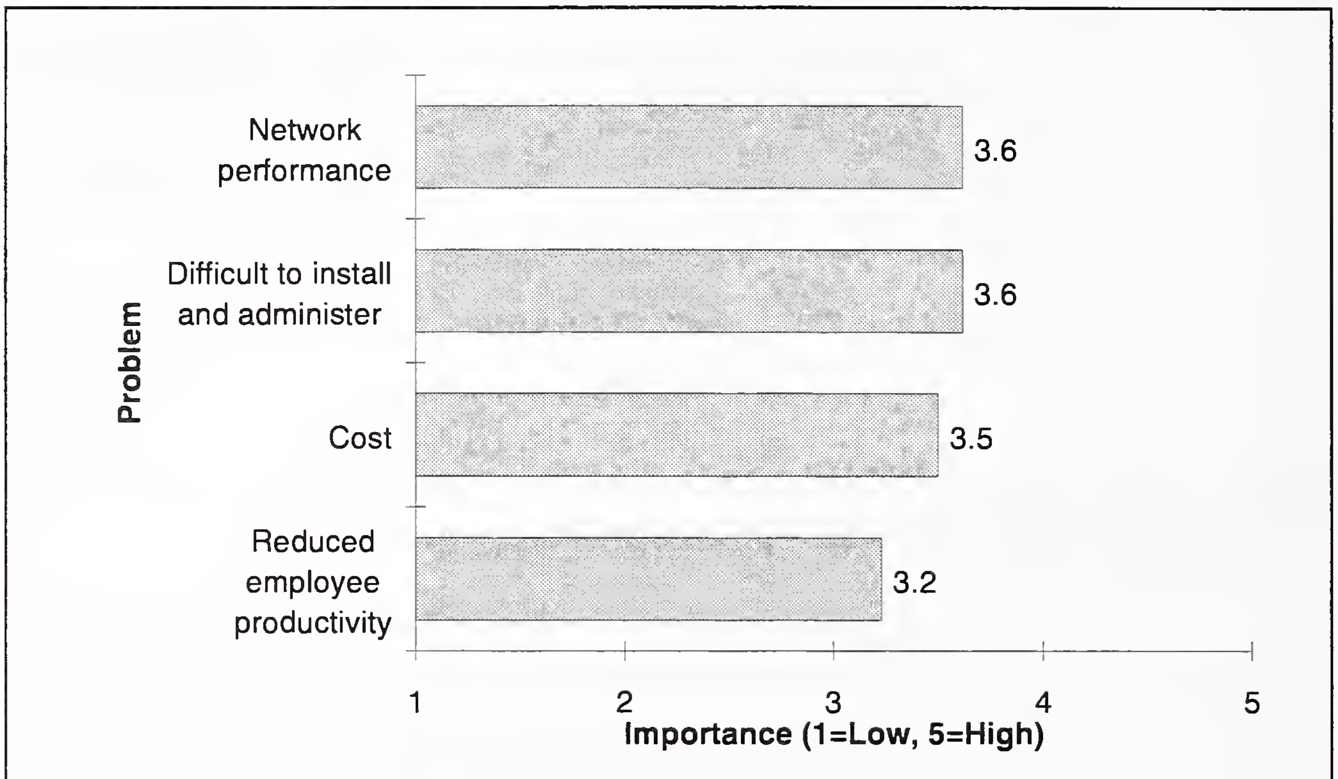
The International Computer Security Association's motto is that "security is not a one-time event. It is a continual process." No matter how effective the software tool, fundamentally security relies upon continual monitoring of audit logs, continually staying aware of new security problems and taking corrective actions, and a host of other activities.

Many security experts state that the lack of assurance about security is the greatest barrier restraining the growth of electronic commerce. Typically the focus of security is placed on protocols, but it is necessary to provide security at all levels, including operating systems, network, client, as well as protocols.

Exhibit V-1 details how respondents rated the importance of problems with security software.

Exhibit V-1

Problems with Security Products



Number of Respondents: 52 *Source: INPUT*

Many vendors are working to provide security packages that are less labor intensive and easier to administer. Platinum Technology, based in Chicago, IL, sells a security portfolio called AutoSecure that provides a wide range of multi-platform access control, policy monitoring, and administration, as well as virus protection and database security management products. Computer Associates' Unicenter TNG product line provides a consistent manner for security management of all IT resources, as well as many other monitoring and management functions.

That employee productivity was ranked the lowest of the four items is not surprising since the primary responsibility of the individuals surveyed is for security. Users and their managers are likely to be much more concerned with reduced productivity. There is a trend towards making security products more transparent and eliminating loopholes that users can circumvent.

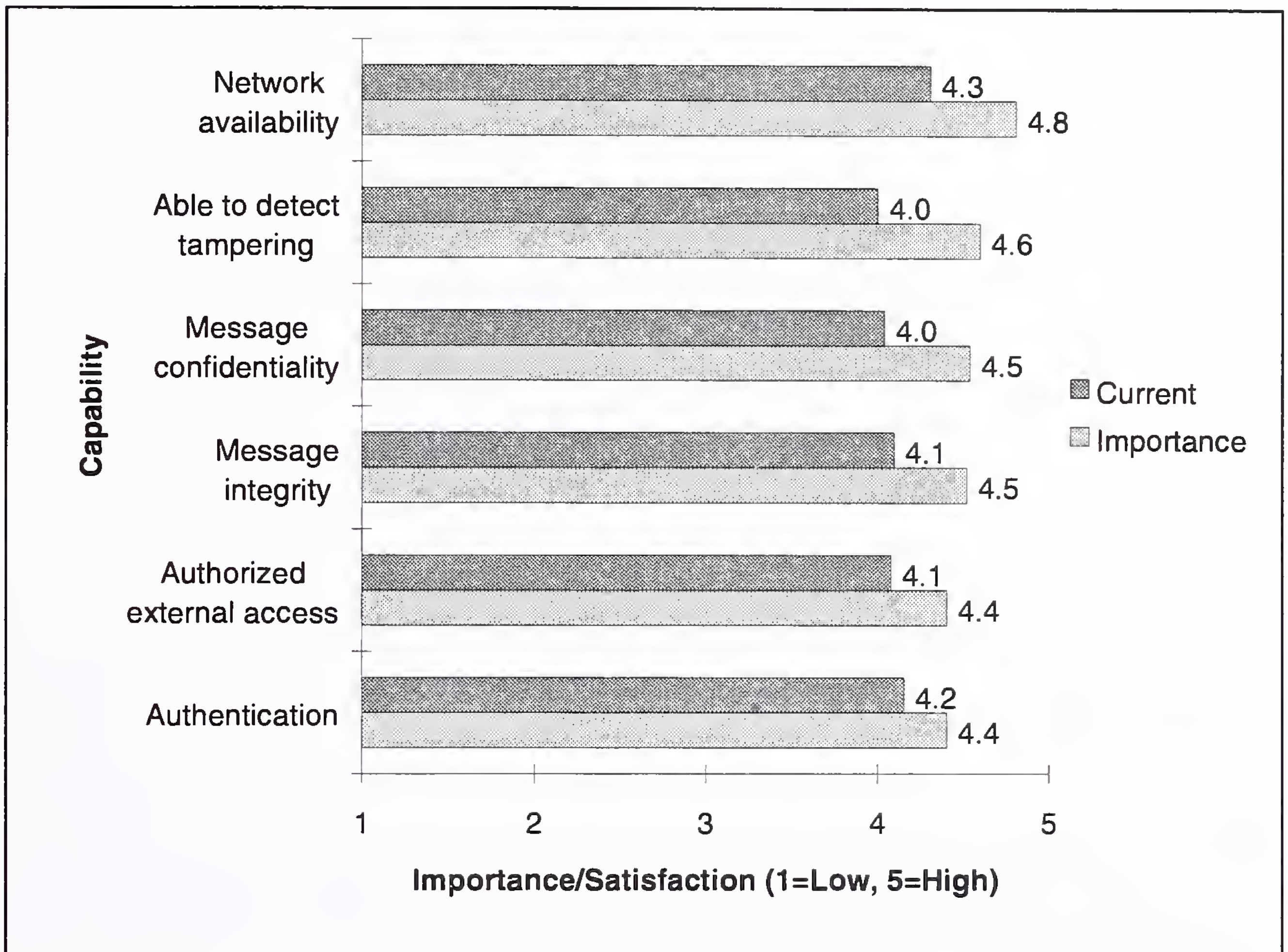
Network performance also had a relatively high importance, yet few vendors are adequately responding to this issue.

B Importance and Satisfaction with Security Solutions

Exhibit V-2 provides a comparison between the importance and satisfaction of current electronic commerce security solutions.

Exhibit V-2

Comparison between Level of Importance and Satisfaction



Number of Respondents: 52 *Source: INPUT*

In comparing the two sets of responses, there is a consistent gap between the expectations of users and the extent to which current products fulfill these expectations. The greatest gap is in the ability to detect tampering, providing message confidentiality and assuring network availability. The smallest gap is in the ability to identify network users.

The fact that respondents ranked authentication highly is interesting because this has been a recurring problem in Windows NT. Additionally, many applications that run on Windows NT and UNIX also have authentication problems. In many cases, users may have a false belief regarding the level of security of their system. For example, in late 1996, researchers conducted a systematic survey of 1,700 sites on the Internet and found that over 60% could easily be broken into or destroyed.

Insuring message integrity and confidentiality is typically accomplished by using encryption technology. The U.S. government has sought to restrict encryption technology with longer than 40-bit key lengths from being exported, with the exception of banking applications. But the need for providing a high degree of assurance of message integrity and confidentiality has spawned hundreds of European companies providing 128-bit and longer encryption keys.

What will be the short-term effect of this policy by the United States government? Whitfield Diffie, the father of public key encryption states, "Can cryptography can be effectively regulated? I think that governments cannot achieve the objectives they say they have or the objectives I believe they really have...but I think that they can do a lot of damage to both democracy and business in the process." In the meantime, in 1998 it was estimated that there are over 500 non-U.S. encryption products.

Brokat Information Systems Java-based technology is being used by many banks to secure their transactions over the Internet. Currently 80% of German banks, many Swiss banks, the largest U.K. banks, and banks in Singapore, Australia, Hong Kong, and Luxembourg use their technology. While a user's browser may normally only support 40-bit encryption, Brokat's technology downloads a Java applet allowing 128-bit encryption to be performed. This effectively bypasses attempts by the United States government to restrict encryption technology.

With respect to detecting tampering, there are a wide variety of tools for auditing system configurations to verify that files are properly configured with the proper permissions. Various system integrity checking and auditing tools examine system files to determine if unexpected or unauthorized changes have been made. These tools also log and organize system events to facilitate quick detection and response to attacks. Many newer tools filter this information to avoid overwhelming the administrator with extraneous information. While these tools can be very effective, they need to be used in a routine and systematic manner.

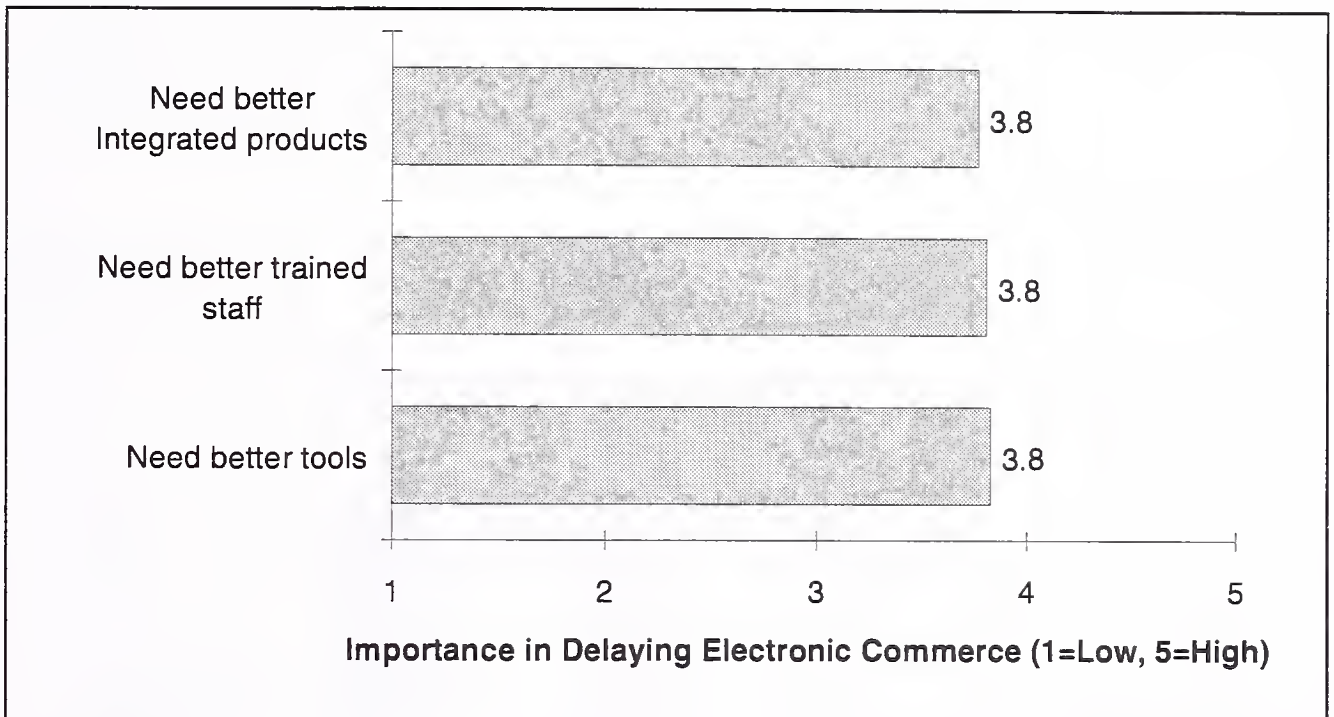
Intrusion detection applications can monitor systems and trigger alarms when security violations occur, but typically are costly and labor intensive, and often have a significant impact on performance. For example, Security Dynamics provides a variety of intrusion detection software to assess the effectiveness of an organization's security, as well as real time checks for security violations.

C
Factors Delaying Electronic Commerce

Exhibit V-3 examines which factors were delaying or inhibiting the implementation of electronic commerce:

Exhibit V-3

Factors Delaying Electronic Commerce



Number of Respondents: 52 *Source: INPUT*

It is interesting to note that users were unable to place a priority on any of the above factors for delaying the implementation of electronic commerce. This chart indicates that while there is an overall belief that these factors are retarding acceptance, management has been unable to clearly establish the decision-making framework to directly address this challenge. This suggests that vendors who position themselves as "your security partner in helping make electronic commerce happen," could achieve a significant market position. Additionally, vendors who provide product education classes and seminars could obtain a competitive advantage in the market. Since respondents feel that they are not in complete control, vendors could promote the messages that their products help users maintain stability and protection over their information systems.

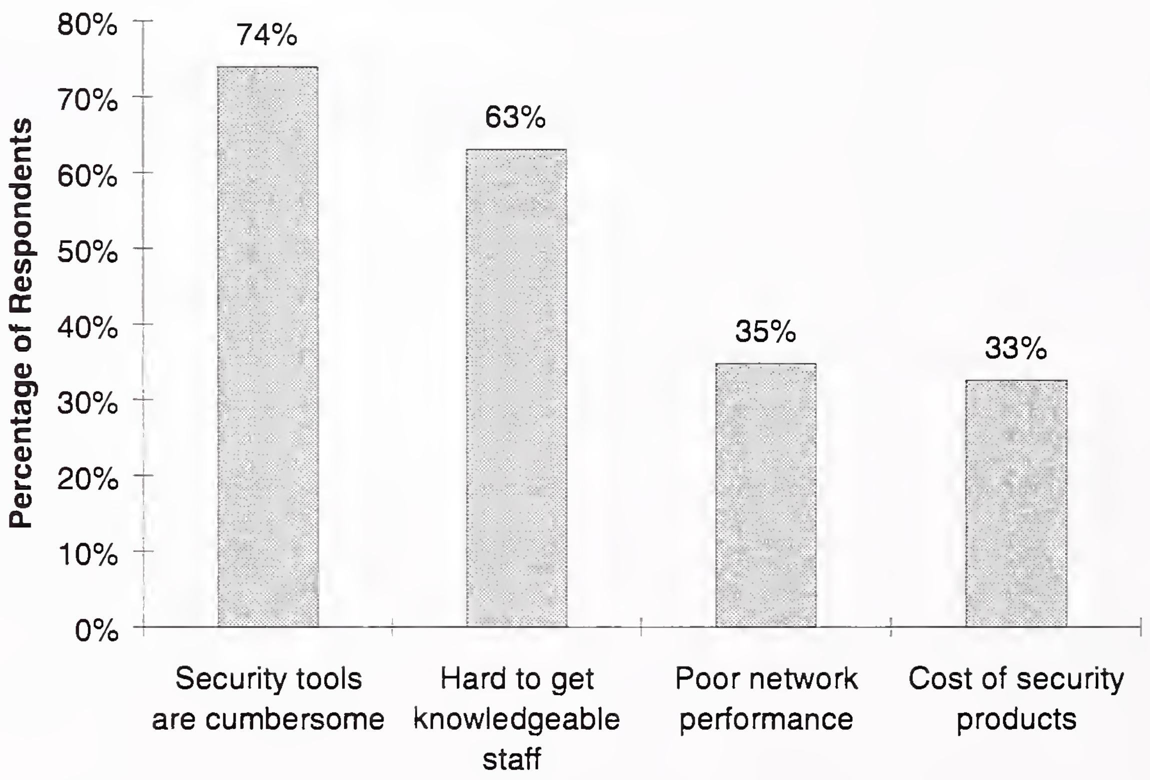
Many companies are seeking to provide better-integrated products. For example, Tivoli, acquired by IBM in 1996, has subsequently been merged with Unison Software and Software Artistry. The product lines of the companies are being integrated and merged together, providing a diverse collection of enterprise wide management, monitoring, scheduling, and security products.

To improve the interoperability of different security products, Intel's Common Data Security Architecture (CDSA) is being adopted by Entrust, Hewlett-Packard, IBM, Motorola, Netscape, and Sun Microsystems. It is hoped that this standard will facilitate the development of security applications that are interoperable, extensible and offer cross-platform support. It is believed that CDSA offers flexible and configurable use of cryptography, certificate management, trust policy management, key and certificate lookup, storage and retrieval, and optional commercial key recovery.

Exhibit V-4 examines which service needs are being unmet or poorly served in the electronic commerce security market.

Exhibit V-4

User Needs that Are Unmet or Poorly Served



Number of Respondents: 48

Source: INPUT

Users find existing tools to be complex, difficult to learn and use, making it difficult to identify, attract, train, and retain staff knowledgeable in their use. Companies such as Security Dynamics (SecurSight) and BrainTree are trying to provide enterprise wide security management systems that provide a single, common interface for controlling and administrating various aspects of security, ranging from authentication, certificates, to encryption.

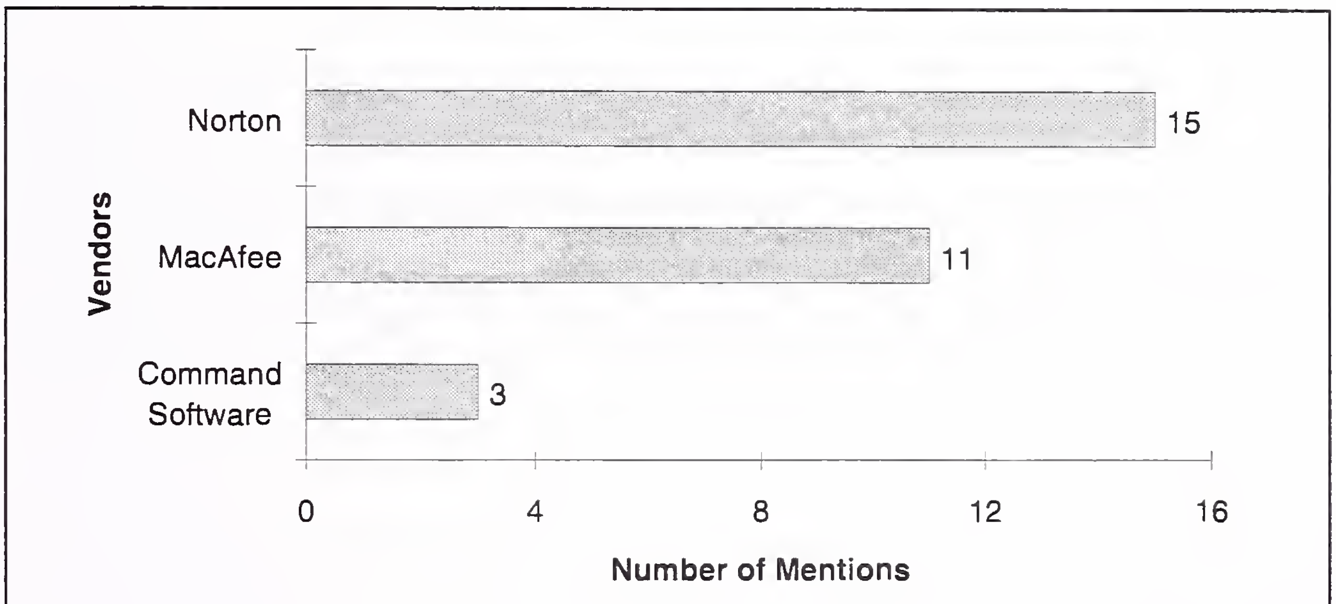
D
Electronic Commerce Security Products Used

Detailed lists of the vendors used by respondents were difficult to obtain. This could be due to respondents' belief that this represented need-to-know information. However, respondents were willing to provide information on virus detection vendors.

In Exhibit V-5, two companies, Symantec and MacAfee (now Network Associates) accounted for 57% of the responses for virus detection products.

Exhibit V-5

Virus Detection



Number of Respondents: 46

Source: INPUT

For all other product questions, 15 or fewer respondents answered. With respect to PC access control, system software from Microsoft and Novell was most often cited. For minicomputer and mainframe access control, system software from IBM, Digital, Netscape and Computer Associates was identified.

For power backup, one-third of the respondents cited the use of generators; the others all used some form of UPS (uninterruptible power supplies). A total of 24 respondents cited the use of firewalls, of which one-third indicated that they were using Checkpoint as their vendor. (Note: see INPUT's report on "Evaluation of Internet Firewall Solutions" for more information on this product category.)

With respect to the other security product categories, a high percentage of the remaining responses were for products supplied by large companies such as Compaq, IBM, Microsoft, Novell, and Symantec.

VI

Security Purchasing

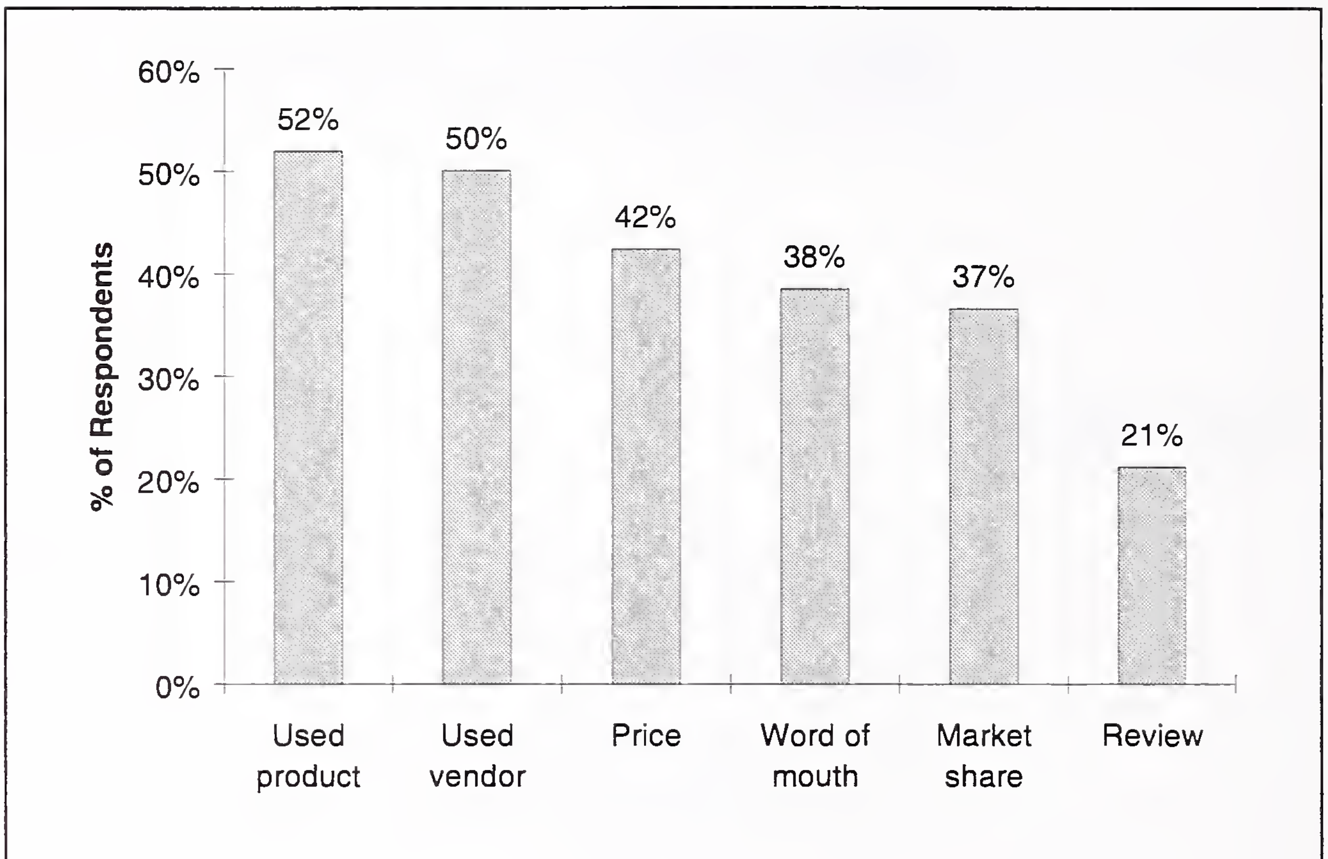
A Vendor Selection

There are over a thousand electronic commerce security products on the market in 1998. As previously mentioned, many of these products are from European companies, providing products with encryption key lengths longer than the 40-bit maximum that the U.S. government imposes on its domestic companies for export. U.S. electronic commerce security companies have a severe competitive handicap selling internationally against European competitors.

The criteria by which users select products among these myriad vendors is shown in Exhibit VI-1.

Exhibit VI-1

How Security Vendors are Chosen



Number of Respondents: 52

Source: INPUT

Prior uses of the product or vendor were the most important criteria, while relatively little influence was given to reviews, word of mouth referrals enjoyed a much higher level of credibility. This suggests that seminars and other ways of achieving face-to-face contact with the customer will have superior value to print media in establishing credibility. While price has importance, it is a secondary consideration after other product characteristics, as supported by Exhibit VI-2.

Why do reviews have such low credibility? This may be due to first hand market experience. For example, Microsoft has marketed Windows NT as being more secure than Unix. But in fact, Windows NT is technologically immature compared to Unix, and has been found to have numerous security bugs.

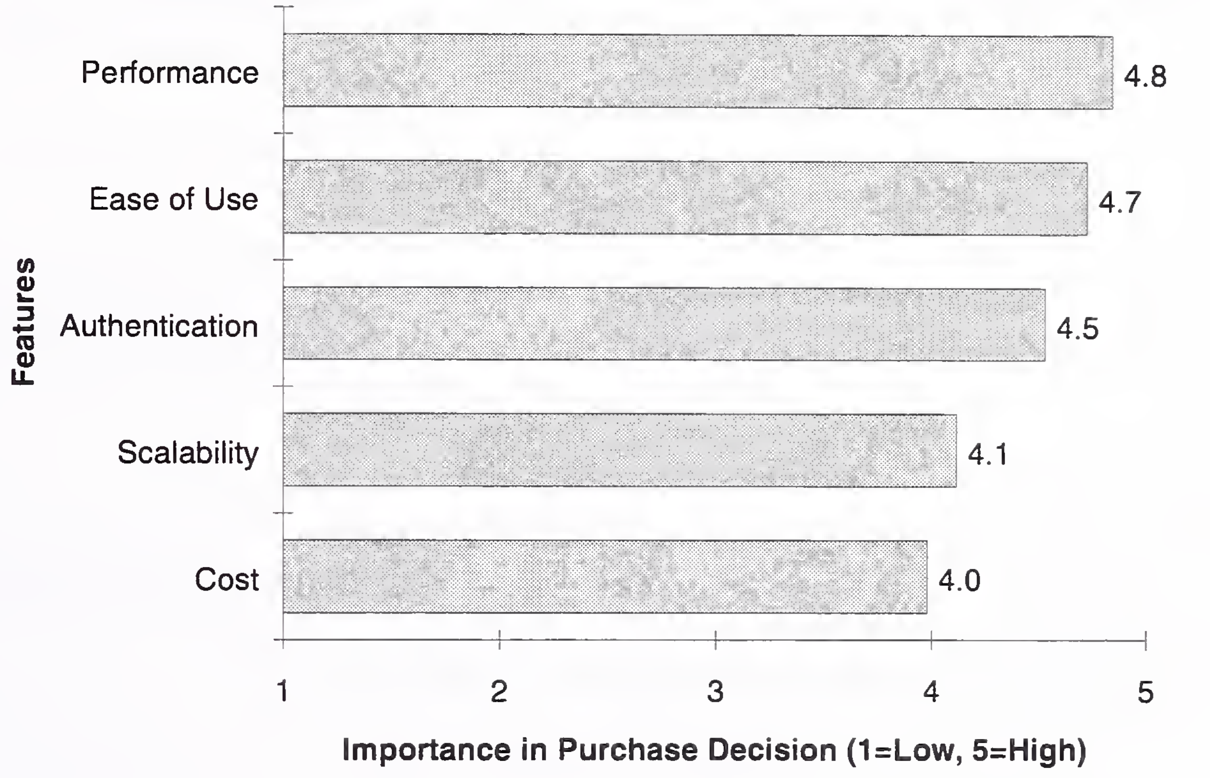
The value of market share suggests that the industry trend towards consolidation will benefit companies such as Network Associates, and work to the disadvantage of companies with less market presence.

B
Key Product Characteristics

Exhibit VI-2 shows the most important aspect of electronic commerce security.

Exhibit VI-2

Importance of Electronic Commerce Security Product Features



Number of Respondents: 51 *Source: INPUT*

The importance of performance may be attributed to the characteristic that the cryptography algorithms used to encrypt and decrypt information requires a significant amount of computation. This problem is being addressed by companies such as Ncipher, who are providing cryptographic accelerators that improve cryptographic performance between 10 to 100 times, depending on the power of the server processor. Ncipher provides support for a variety of Unix and Windows NT systems, as well as applications from Apache, Microsoft, Netscape and many other vendors.

Ease of use is a problem for many security products such as packet filter firewalls. These products are not able to do selective filtering, perform "variable logging," or do user authentication. This can result in substantial security administration overhead in monitoring audit logs.

Some vendors are addressing this problem by the use of smart filter firewalls that use heuristic rule checking to avoid conflicting rules, provide authentication, and track session state.

There did not appear to be any correlation between the importance of these features and company size.

C
Electronic Commerce Security Industry Trends

The electronic commerce security industry consists of a wide and diverse collection of products, including:

- Virus detection
- Access control (PC, minicomputer, mainframe), sign-on software, hardware security devices, terminal key locks, biometrics, signature verification
- Firewalls
- Encryption (data and communications), public-key cryptography
- Dial-back / secure modems
- Security evaluation software, business continuity planning software.

Industry Consolidation

Consolidations, mergers and alliances in the electronic commerce security market have marked the past year. While Network Associates and Security Dynamic Technologies have been the most active companies in assembling a complete product offering, many other firms appear to be executing similar strategies, and thus further consolidation can be expected.

Network Associates was formed as a result of the merger between McAfee Associates and Network General. Subsequently, Network Associates has acquired Pretty Good Privacy (encryption and authentication), Trusted Information Systems (firewalls), Secure Networks Inc. (security vulnerabilities), and Dr. Solomon (virus software).

Some of the other notable industry mergers and acquisitions are:

- Security Dynamics Technologies has acquired RSA Data Security Inc., (encryption technology), Intrusion Detection Inc., and DynaSoft SA (authentication products).

- Axent Technologies acquired Raptor Systems Inc., (firewall) and AssureNet Pathways Inc.,

- Check Point Software Technologies, the leading independent provider of firewalls, acquired MetaInfo Inc. (address management software).

- Cybercash merged with ICVERIFY (electronic money).

Users should examine closely the claims by vendors that their product lines are consistent and well integrated. Providing such integration often requires considerable time and effort and is difficult to accomplish by firms undertaking rapid acquisitions.

System companies such as IBM and Sun Microsystems are examples of firms that have been actively working to integrate and make transparent, various elements of security technology in their products. For example, Sun enables companies to implement virtual private networks across the Internet by providing transparent encryption and decryption at gateway nodes by using its Solaris SunScreen SPF-100 network security system.

There have also been significant alliances, such as IBM and Equifax's, effort to offer digital certificate services that will verify the identity of customers making transactions or sending email.

Development and Growth of European Encryption Industry

As described elsewhere in this document, the European encryption industry which did not exist five years ago, has become a large and flourishing industry, largely due to efforts by the U.S. government to restrict domestic companies from exporting encryption technology having greater than 40-bit key lengths. Some of the most notable European electronic commerce security companies are Brokat Informationssysteme GmbH, Baltimore Technologies Limited, and Sapher Servers Limited.

Trusted Systems

There have been considerable efforts by firms such as Data General, Hewlett-Packard and Sun Microsystems, to market their trusted operating systems as software that enables providing electronic commerce systems with a higher degree of assurance that they will function in a secure manner. Originally developed to meet government defense requirements, these firms are targeting vertical commercial markets that have explicit needs to assure that data remains private and secure.

A

User Questionnaire

Study Title: ______________________________

Type of Interview:

□ Vendor □ Telephone

□ User □ On-Site

□ Other □ Mail

Company: ______________

Address: ______________

____

____

____

City/State: ______________

Zip: ______________

Telephone: ______________

Fax #: ______________

Project Code/Catalog No. ______

Interviewer Initials ______

Interview Date. ______

QC Initials ______

QC Date ______

Data Entry Initials ______

Data Entry Date ______

Company Type: ______

Annual Revenue: ______

# Employees: ______

Total IS Budget: ______

Total # IS Staff: ______

Respondent(s):

Name Title Phone/Ext.

Role in Project:

Referrals:

Industry (User Interviews Only):

	Discrete Mfg.		Wholesale		Federal Government		Process Mfg.
	Banking/ Finance		State & Local Government		Transportation		Insurance
	Consumer/ Home		Utilities		Medical		Other Industry Specific
	Communications		Services		Cross-Industry		Retail
	Education						

This survey is to determine your satisfaction with, and improvements you would like in the provision of electronic commerce security. This includes *firewalls, virus protection, encryption, and access control.* The survey will also enable us to analyze how best practice is developing within electronic commerce security.

Important (this survey covers a sensitive issue) – Your responses to the questionnaire will be kept in strict confidence and will not be released to any party. All responses will be aggregated, and none will be attributed to individual respondents.

You will be provided with an executive summary of the results of this survey.

1. Are you the person who is most able to evaluate the use of electronic commerce security on behalf of your organization? If not, to whom should I speak? (Close the interview and contact the specified person.)

Collect related demographics

2. What is your role?

____

3. To what will you refer in your answers? (Check one)

Your site (is corporate HQ) ❐
Your site (is not corporate HQ) ❐
Your company nationwide (all sites in country) ❐
Your company worldwide ❐

4. Would you give us any rough idea of the amount or value of electronic commerce performed by your company?

Web site in hits/day ______
EDI in transactions/day ______
Value of product purchased per day $______
Other: (State) ____________________________________ ______

5. What areas of electronic commerce do you see growing at your company over the next year? By how much?

	0-25%	26-50%	51-75%	+76%
Email	❐	❐	❐	❐
EDI	❐	❐	❐	❐
Web-based storefront	❐	❐	❐	❐
Other __________	❐	❐	❐	❐
Don't know	❐			

6. What electronic commerce security services are you using, or plan to use in the future?

	Current	Future
Internal certificate server	□	□
External certificate server	□	□
Value added network	□	□
Encrypted email	□	□

7. How much experience do you have in matters relating to electronic commerce security? (Check one)

Less than one year	□
1 to 2 years	□
2 to 3 years	□
4 to 5 years	□
Over 5 years	□

8. Did you acquire any of this security experience prior to your current job?

Yes □

9. How valuable would you rate the following (on a scale of 1-5) for helping minimize electronic commerce security risks? Indicate if this is something you currently do.

	Rating (1-5)	Do?
Developed security policy	______	□
Security consultants	______	□
Use software to systematically identify vulnerabilities	______	□
Periodically do random checks to check security procedures	____	□
Other: (State) ______________________________		□

10. How critical, on a scale of 1 to 5, would you rate the following security violations? How difficult would you rate, on a scale of 1-5, the measures needed to prevent their reoccurrence?

	Importance	Difficulty
Users could not make use of system	______	______
Databases / web accessed without authorization	______	______
Fraudulent transaction	______	______
Unauthorized user	______	______
Other: (State) ______________________	______	______

11. With respect to your IT budget:

What is your total IT budget? $______
What percentage goes for providing security? _______%
What % of the security budget is for client protection? _______%
What % of the security budget is for gateway/firewall prot.?____%
What % of the security budget is for server/host protection?____%
What % of the security budget is for internal personnel _______%
What % of the security budget is for external personnel _______%

12. On a scale of 1-5, how important to your company are the following problems that you've experienced with your security products.

Difficult to install and administer ______
Cost ______
Network performance ______
Reduced employee productivity ______
Other: (State) ____ _____

13. It has been suggested that a sizable percentage of actual security violations come from employees, ex-employees and vendors who have access to security information. In your experience, what percentage of electronic commerce security violations at your company come from:

	0-25%	26-50%	51-75%	+76%
Current employees	□	□	□	□
Ex-employees	□	□	□	□
Vendors / ex-vendors	□	□	□	□
External, unknown	□	□	□	□
Don't know	□			

14. Rate the importance of the following aspects of electronic commerce on a scale of 1-5, and rate, also on a scale of 1-5, how well current products you are using address them.

	Importance	Current
Network availability	______	______
Able to detect tampering or interference	______	______
Able to identify network users	______	______
Message confidentiality	______	______
Message integrity	______	______
Authorized external access	______	______

15. How do you choose your security vendors? (check all that apply)

Product's market share □
Review or article in magazine □
Word of mouth / recommendation □
Have worked with vendor before □
Have used product before □
Price □

16. How strongly, on a scale of 1-5, do you feel the following are delaying or inhibiting the implementation of electronic commerce?

Need better tools to analyze and monitor security ______
Need better trained and larger staff ______
Need better integrated and more transparent products ______
Other: (State) ______

____

17. What services needs are unmet or poorly served in the electronic commerce security market? Check all that apply.

Hard to identify, attract and retain knowledgeable staff □
Many security tools are too cumbersome □
Network performance is adversely effected □
Cost of security products and services needed is prohibitive □
Other: (State) ______________________________ □

____

18. What types of attacks have you experienced? Check all that apply.

Denial of service □
Sendmail attacks □
Port scanning □
IP spoofing □
Mail bombs □
Other: (State) ______________________________ □

____

19. By what percentage will you increase your IT security budget over the next year to prevent these attacks in the future?

10% or less □
11% to 25% □
26% to 50% □
51 to 100% □
Over 100% □

20. With respect to products used to insure electronic commerce security, how would you rate (on a scale of 1 to 5), the importance of the following?

Ease of use ___
Performance ___
Authentication ___
Cost ___
Scalability ___
Other: (State) ______________________________

21. How would you rate (1 to 5), the importance of security in electronic commerce with respect to the following departments in your company?

Finance
Manufacturing ____
Sales / marketing ____
Administration / corporate management ____
Customer service / support ____

22. Following is a list of various types of security software. For each type, please state the following: Name of current security software vendor if you know it; the names of other vendors you are aware of; Rate on a scale of 1-5 the effectiveness of your current vendor; If you do not currently use software of the type, indicate if you plan to do so in the future.

Type of Security Software	Name of Current Vendor	Effectiveness of Current Vendor (1-5)	Plan to Use in Future (check)
PC access control			
Mini/mainframe access control			
Redundant communications or power backup			
Dial back or secure modems			
Firewalls			
PC hardware security devices			
One-time (token-based) passwords			
Terminal key locks or lock words			
Data encryption			
Single sign-on software			
Telecommunication encryption			
Signature verification			
Security evaluation software			
Message authentication codes			
Business continuity planning software			
Public-key cryptography			
Biometrics to authenticate users			