

The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

An RSA Security Survey

At a time when there is great concern about the security of information technology, few people have a more informed perspective on this critical topic than Chief Security Officers (CSOs). From their unique vantage point, CSOs are equally attuned to global and national security trends, enterprise security strategies and the daily threats, large and small, that assail their own networks.

To find out what CSOs are thinking — and what strategies they're pursuing — RSA Security commissioned an independent survey, which was conducted during April and May 2003. More than 250 readers of CSO magazine were asked a series of questions relating to their concerns about security and their organizations' responses to security threats. A significant portion of the questions relate to how organizations protect sensitive consumer and employee information and how they validate the identities of online users.

The survey results are presented here, along with commentary on the events that RSA Security believes have influenced CSOs' viewpoints. In some cases, we have also compared CSOs' answers to those provided by consumers who took part in a similar RSA Security-sponsored survey during the same time period.

This paper then concludes with a discussion of some of the technologies that RSA Security brings to the table, with a focus on solutions for identity and access management (I&AM) and encryption.

Job titles of those participating in the survey included Chief Security Officer, Director of Security, Chief Information Officer, VP of Operations, Director of IT and other titles. For the sake of convenience, participants are jointly referred to as CSOs or security professionals.



The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

Table of Contents

I.	Which of the following has had the most impact on your company's awareness of security issues?	1
II.	Which of the following [threats] is your organization most likely to experience?	2
III.	Which of the following [threats] would have the most impact on your organization?	3
IV.	In the past six months what measures has your organization taken to increase security?	4
V.	In the past 18 months, has increased sensitivity toward security caused your organization to change any of the following?	4
VI.	Has increased attention to security resulted in you personally altering any of the following behaviors?	5
VII.	Rate the sensitivity of customer information within your organization.	5
VIII.	Rate the sensitivity of employee information within your organization.	6
IX.	Rate information security measures based on prevalence.	6
X.	Rate information security measures based on effectiveness.	8
XI.	Rate the following information security measures by their impact on the future of information security.	8
	RSA Security: A CSO's Natural Ally	9
	A Vision for the Future	10
	A Final Thought	10

The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

I. Which of the following has had the most impact on your company's awareness of security issues?

The September 11 Terrorist Attacks

More than any other event or trend, the September 11 terrorist attacks loom large in CSOs' consciousness. Questioned more than 18 months after those devastating events, 30% of security professionals said the attacks have had the most impact on their company's awareness of security. No doubt, there is a strong personal dimension to this response. Like everyone else, CSOs witnessed the attacks from the perspective of private citizens. Later, they were also likely to have viewed the attacks through a professional lens, grimly noting how a catastrophic event can decimate an organization's physical and technology infrastructure.

Additionally, the attacks triggered governments and industry around the world to rethink security at the highest levels. Prompted by initiatives such as the U.S. National Strategy to Secure Cyberspace, large enterprises have begun to address the gaping vulnerabilities that developed, unchecked, during the explosive growth of the global network.

Government Regulation

In stark contrast to the catastrophic nature of the September 11 attacks, the second most commonly cited source of security awareness is the advent of new government regulations, mentioned by 24% of those surveyed. New laws, many of them created in response to the explosion of identity theft, require organizations to protect sensitive consumer and business data from being stolen or otherwise compromised. (See the sidebar, "It's the Law".)

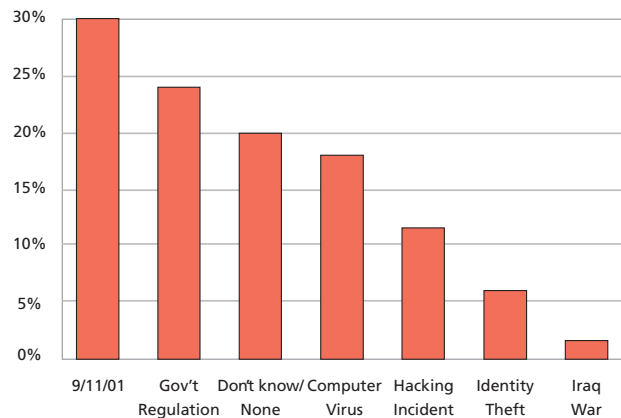
Often, this responsibility falls on IT security professionals. For example, in response to the Health Insurance Portability and Accountability Act (HIPAA) — which is designed to protect patient health information — many healthcare organizations have implemented more secure methods for authenticating online users who need to access applications from outside the network.

Global Viruses

18% of respondents indicated that computer viruses had the greatest impact on their awareness — and with good reason. Attacks via viruses and worms continue to grow in frequency, virulence and efficiency. For example, the Slammer virus — which struck in January 2003 — spread hundreds of times faster than its famous predecessors, Code Red and Nimda. On being launched, millions of Slammer clones started attacking computers at random, and within three minutes, the number of replicants was doubling every 8.5 seconds. In the future, some experts predict, powerful "flash worms" will do significant damage within seconds of being released.

Adding to the threat, many viruses and worms now incorporate multiple attacks: unleashing a deluge of phony e-mail; installing "back doors" on target systems, which later

Which of the following has had the most impact on your company's awareness of security issues?



allow a system to be commandeered to participate in denial of service (DoS) attacks; and installing keystroke loggers, which capture passwords and identity information and send it to a data collection point, facilitating identity-related crimes.

The indirect costs of worms and viruses can be prohibitive. Worldwide cleanup costs for a single virus frequently exceed \$1 billion and occasionally cost several billion.

Hacking Incidents

12% of those surveyed said that hacking incidents had the greatest impact on their awareness. Hacking often results in the theft of valuable information such as new product designs or business plans. It can also lead to the disruption of critical infrastructure. For example, in Australia, a disgruntled contractor managed to work his way through network defenses at a sewage treatment facility and released 800,000 liters of raw effluent.

Identity Theft

Only 6% of CSOs said that identity theft had the greatest impact on their awareness of security issues. This low level of concern is somewhat surprising given that identity theft is projected to cost U.S. businesses \$48 billion during 2003. The CSO response is also noteworthy for how it contrasts to consumers' views. In a survey of consumers that asked similar questions, 22% of respondents said that identity theft had the greatest impact on their awareness of security.

According to the Federal Trade Commission, more than 10 million Americans were victims of identity theft during the past year, suffering losses that totaled \$5 billion. Many victims are forced to spend significant time and financial resources restoring their credit reputation. The disparate perspectives of consumers and CSOs are worth contemplating. Organizations may want to heighten their focus on identity theft, knowing it is such a vital concern to their customers.

The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

It's the Law

A growing body of laws and regulations are creating new demands on IT security professionals. Some of the most noteworthy of these are summarized below.

- Disclosure of identity theft and related fraud. The California Data Security Act will require enterprises that do business in California to disclose to California residents any time their unencrypted personal information has been compromised. The law does not mandate data encryption. However, it is expected that many organizations will be motivated to encrypt their information.
- Protection of Social Security Numbers. The California Law on SSN Confidentiality will prohibit companies from using SSNs as passwords for logging into web sites and will forbid the transmission of SSNs over the Internet unless the connection is secure or the number is encrypted.
- Protection of health and personal information. The federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 defines standards for safeguarding the privacy and security of medical records and other individually identifiable health information.
- Protection of personal financial information. The Gramm-Leach-Bliley Act defines requirements for financial institutions to protect the privacy and security of customers' personal financial information.
- Transmission of personal data across borders. European Commission Directive No. 95/46 sets standards for ensuring adequate protection of personal data that is transferred from E.U. countries — which have rigorous privacy requirements — to non-E.U. countries.
- Use of electronic signatures to authenticate online transactions. Numerous laws govern the use of electronic signatures as a means of authenticating documents and transactions. These include the EU Directive on Electronic Signatures, the Japanese Law Concerning Electronic Signatures and Certification and others.

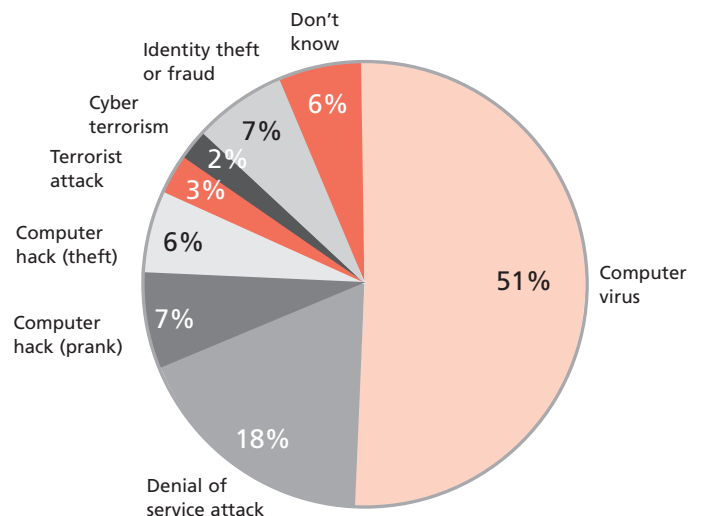
II. Which of the following is your organization most likely to experience?

CSOs are clear about what kinds of threats they are most likely to face, with computer viruses — mentioned by 50% of respondents — topping the list by a wide margin. Viruses and worms have become an ugly fact of life, with “writers” and security experts locked in an ever-escalating battle.

18% of the CSOs identified denial of service attacks as the next most likely threat. While numerous DoS attacks have targeted individual companies, this high level of concern may be based on a specific incident with far-reaching implications: a massive and highly coordinated distributed DoS attack in October 2002 that nearly succeeded in bringing down the Internet. Many observers believe that such attacks will recur, with the attackers using increasingly sophisticated and effective techniques.

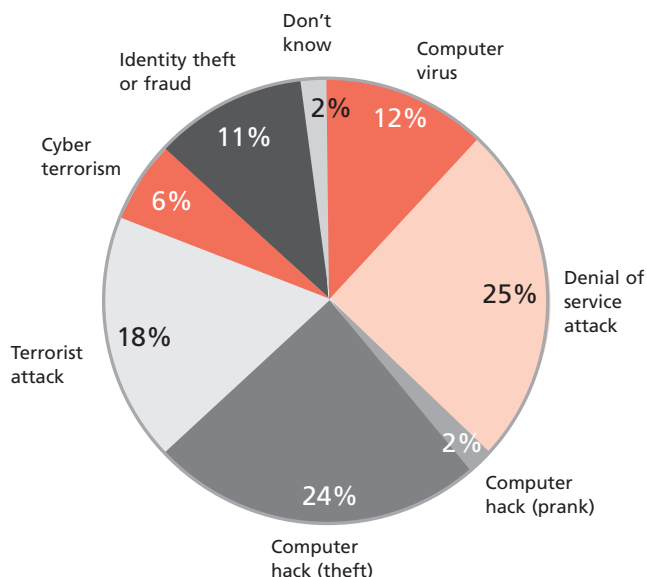
13% of those surveyed view computer hacking — whether as a prank (7%) or for purposes such as information theft (6%) — as being the most likely threat. Needless to say, hackers have victimized many organizations, with high-profile companies and government agencies making especially inviting targets. While terrorist acts and cyber terrorism can be as damaging as some of these other types of threats, they are viewed as being far less likely to occur.

Which of the following is your organization most likely to experience?



The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

Which of the following would have the most impact on your organization?



III. Which of the following would have the most impact on your organization?

Faced with a wide range of potential threats, CSOs were divided over which would have the most impact on their organizations. 25% indicated that a Denial of Service attack would have the most impact, while 24% said computer hack related to information theft and 18% cited a terrorist attack.

DoS Attacks

A successful DoS attack on a business can bring operations to a standstill by bombarding the network with illicit traffic, thus choking off legitimate traffic. The costs may include lost employee productivity, lost sales and opportunities as a result of disabled web sites and negative publicity. In one well-known case, online traffic intended for a leading office supplies merchant was diverted to a competitor site, resulting in a direct loss of revenue.

While a focused DoS attack may affect one company or a handful of targeted companies, a truly massive attack could potentially bring down the Internet, with enormous ramifications for nations, economies, enterprises and individuals. Many observers believe this was the intent of the October 2002 attack on the Internet's 13 Domain Name Service (DNS) root servers, which translate domain names into IP addresses. While the attack ultimately failed, due to design redundancies, there was speculation that it would not be difficult to intensify an attack sufficiently to shut down the global network.

Hacking Incidents

A computer hack that results in information theft was also ranked as a serious threat, because it can result in the loss of sensitive and/or valuable information. For example, several leading software firms have been victimized by hackers who steal source code for new or widely used products and post the code on public web sites. Similarly, in October 2003, the source code for a yet-to-be-released version of a popular online game was stolen and posted. This enables gaming "cheaters" to develop their own attacks and weapons, giving them an unfair advantage and distorting the game experience for millions of users. Such incidents are damaging, both to a company and its customers.

Identity Theft

While only 11% of CSOs singled out identity theft as having the greatest impact on their organizations, it should be remembered that the theft of customer or employee data is, in many cases, a subset of the category "hacking with the intent to steal information," the second most frequently mentioned threat. Cases of large-scale identity theft are increasingly common. Some examples:

- 30,000 consumer credit reports were stolen from a credit-reporting agency, resulting in \$2.7 million in losses to credit issuers.
- 265,000 Social Security numbers (SSNs) were stolen from a database of California employees, including the governor and state legislators.
- 8,000,000 credit card numbers were stolen from a company that processes merchant transactions.

Worldwide, identity crimes will cost an estimated \$221 billion in 2003. In addition to the resulting financial losses, companies that fail to protect consumer data may face increased scrutiny by regulators and investors, increased security costs to repair the security breach and lawsuits filed by angry victims of identity theft.

Terrorist Attack

18% of CSOs said that a terrorist attack would have the greatest impact on their organization. One can probably assume that this group was envisioning either a catastrophic event, on the scale as the 9/11 attacks, or a smaller attack that directly affected their own people and facilities. In either scenario, a business can be debilitated or, in extreme cases, destroyed by the loss of life, destruction of property and disruption to business operations that result from such an event.

Cyber Terrorism

While only 6% of CSOs indicated that cyber terrorism is likely to have a major impact on their organizations, this lack of concern may simply be based on the fact there has not yet been a successful Internet-based global attack. However,

The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

many suspicious intrusions have been reported worldwide by water treatment facilities, aviation flight control systems, dam owners and managers of power grids and telecommunications systems. Additionally, network attacks have been used in regional disputes, including the Arab-Israeli conflict and the conflict between India and Pakistan over Kashmir.

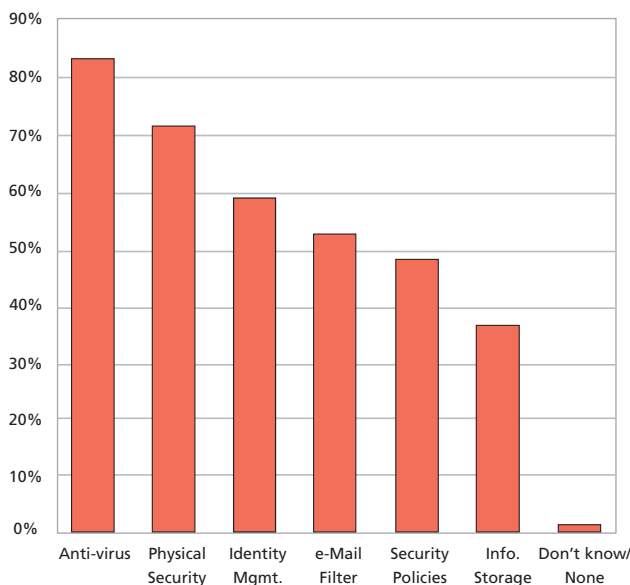
IV. In the past six months what measures has your organization taken to increase security?

Well aware of the risks they face, CSOs are not standing idly by. Responses to this question suggest they are moving on many fronts to combat security threats. 84% said their organization had installed or upgraded antivirus software during the previous six months. As routine and inexpensive as this measure may seem, it is an essential practice, given the accelerating pace of virus attacks and their increasing efficiency.

59% of respondents said their organization had implemented more advanced forms of identity and access management — suggesting that password protection is being gradually supplanted by more robust methods. This inference is borne out by other data from the survey, which shows significant use of encryption, token-based authentication and web access management, alongside traditional password protection. (For details, see question IX.)

53% of CSOs reported that their companies had added an anti-spam e-mail filter in the prior six months. This measure addresses the double threat that spam poses: choking the

In the past 6 months what measures has your organization taken to increase security?



network with unwanted traffic and diverting employees from productive work, if only to delete the spam.

48% of security managers said they had reviewed the security policies of their suppliers. In an era when partners are routinely granted access to sensitive corporate resources, there is a growing awareness that security strategies must extend beyond the walls of the enterprise to encompass partners, customers and suppliers. A company that employs best practices to establish trusted user identities for its own employees can be victimized by a partner whose lax measures enable illicit users to commit misdeeds. For example, an insider at an automotive credit company helped his confederates pose as legitimate, corporate customers of a credit bureau, enabling them to steal thousands of consumer credit reports. Needless to say, there's great value in a company's periodically reviewing its own security measures to be sure they reflect current best practices.

V. In the past 18 months, has increased sensitivity toward security caused your organization to change any of the following?

Looking more closely at behavior changes, the survey found that 80% of companies had changed their method of storage or access for customer and employee information during the prior 18 months. This suggests that, while identity theft may not be explicitly at the top of a CSO's agenda, the security measures being put in place have the positive effect of protecting sensitive customer/employee data. While the respondents were not asked to specify what types of changes were made, there are a number of possibilities. These include encrypting databases, implementing more secure techniques for authenticating users who are allowed to access data or managing access privileges more closely through authorization solutions.

25% of CSOs also reported changes in their company's willingness to conduct business online during the prior 18 months — the inference being that organizations are less willing to launch new e-business initiatives. This hesitancy may reflect ongoing concerns about security or poor ROI on prior investments. In either case, the sure result is to slow the growth of e-business until the perceived shortcomings have been addressed.

Asked whether their organizations had changed corporate travel policies during the prior 18 months, a period that almost extended back to September 2001, 47% answered in the affirmative, suggesting that companies continue to exercise caution at a time of heightened concern about terrorism.

The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

VI. Has increased attention to security resulted in you personally altering any of the following behaviors?

Heightened awareness of security threats has led many CSOs to make changes in their personal behavior. Some of these changes align with changes at the corporate level, as described in the previous question. Additionally, when compared to consumer responses on a similar question, it turns out that CSOs are “people of action,” changing their behavior at a higher rate than consumers.

Changes Relating to Online Transactions

Interestingly, the professionals who are responsible for ensuring the security of e-business clearly have some doubts about the safety of doing business online. 43% of CSOs said they had changed their practices for providing online merchants with personal information (compared to 25% of consumers who had made a similar change); 28% had changed their behavior when using a credit card for online purchases (compared to 13% of consumers); and 24% had reduced the frequency of online purchases (compared to 13% of consumers).

Not everyone is running for the exits, however. More than a third of the CSOs (35%) said they had made no changes at all (compared to 30% of consumers). This number might be interpreted in at least three different ways: CSOs have a high degree of confidence in the safety of online transactions; they are either naïve or fatalistic about the security risks; or they don’t transact business online in the first place and therefore have not seen the need to change their behavior.

Responding to a question on physical security, 37% of those surveyed reported that they had made changes in their use of air travel (compared to 19% of consumers and 47% of companies). Although further details were not requested, such changes might take the form of traveling less frequently, flying during off-peak hours or avoiding major airports in favor of smaller hubs (on the theory that flights originating in major cities during peak hours are more likely to be targeted by terrorists).

VII. Rate the sensitivity of the following types of customer information within your organization.

As the guardians of enterprise IT resources, CSOs have a sweeping view of how customer information is gathered, protected and shared within their organizations. Asked to rate the sensitivity of various types of customer data, their responses provide much food for thought.

Sensitivity of customer information within your organization.

	Never Given Out	Highly sensitive	Given out occasionally	Divulged freely	Not at all sensitive
Customer Name	30%	38%	21%	5%	5%
E-mail address	29%	39%	23%	5%	3%
Credit card/ bank account number	78%	19%	0%	0%	0%
Social Security number	73%	22%	0%	0%	0%
Home phone number	66%	28%	3%	0%	0%
Wireless phone number	59%	30%	5%	1%	0%

The Good News

Many organizations recognize that customers’ personal data is vulnerable to abuse and, therefore, requires protection. Social Security numbers — which are often the starting point for identity theft and fraud — are rightly seen as the most sensitive piece of customer information. 73% of respondents said their organizations never give out customers’ SSNs; an additional 22% said SSNs are viewed as being “highly sensitive.” This marks a dramatic reversal from even a few years ago, when SSNs were routinely displayed on driver’s licenses, employee badges and direct marketers’ mailing labels — practices that helped drive the rapid growth of identity fraud.

Enterprises show an even higher level of caution with bank account and credit card numbers, with 78% saying they never give out that information and 19% reporting that they treat it as highly sensitive. Further reflecting a protective attitude toward consumer data, 66% of those surveyed said their firms never give out customers’ home phone numbers while another 28% treat that information as highly sensitive.

Consumers, who show great reluctance to give out their personal information, would certainly view these results favorably. For example, 90% of the consumers surveyed on behalf of RSA Security said they were “not at all likely” or “not very likely” to disclose their SSNs and 51% said they were not at all likely or not very likely to give out their home phone numbers.

The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

The Bad News

Still, the picture is not all rosy. 26% of the CSOs surveyed said their organizations either occasionally or freely divulge customer names to third parties and another 5% said they treat this information as “not at all sensitive.” 31% occasionally or freely divulge customer e-mail addresses or treat the information as not sensitive, no doubt contributing to the epidemic of spam.

These last results call attention to a thorny issue: under what circumstances should organizations be allowed to share sensitive consumer information with third parties? Many consumer advocates believe that such sharing of information — which is often actually a sale of information — should be barred unless the consumer has explicitly given permission to do so. In contrast to this “opt in” approach, many commercial interests prefer an “opt out” approach, which allows them to share/sell information unless the consumer has explicitly barred them from doing so.

Actions Are Just as Important as Attitudes

One final thought on this topic: respecting the sensitivity of consumer information is not the same thing as protecting the information from theft or abuse. Organizations that pay lip service to privacy and confidentiality but do not take steps to ensure the safety of sensitive personal data are putting their customers in harm’s way. Conversely, organizations that deploy effective security technologies and implement best practices will find that security is a significant and highly valued differentiator that sets them apart from competitors.

VIII. Rate the sensitivity of the following types of employee information within your organization.

There are key similarities and clear differences in the extent to which organizations share customer and employee data. Employee Social Security numbers are viewed as having virtually the same level of sensitivity as customer SSNs. 74% of CSOs said their companies never give out employee SSNs (compared to a 73% figure for customer SSNs) and 22% treat both customer and employee SSNs as “highly sensitive.” Likewise there are close similarities in how home phone numbers are treated, with 91% of companies saying they never give out employee home phone numbers or treat them as highly sensitive; the comparable figure for customer phone numbers was only slightly higher (94%).

On the other hand, some employee information is shared more freely than customer information. Employee names are given out occasionally or divulged freely by 52% of responding companies, twice the rate of disclosure for customer names. E-mail addresses are given out occasionally or divulged freely by 53% of organizations, compared to a 28% rate for customer e-mail addresses. While it is possible

to construe these results in a negative light (e.g., employees are second-class citizens when it comes to protection of their personal data) it is more likely that these discrepancies reflect the business need to share employee information with partners in order to facilitate cooperation.

IX. Rate the following information security measures based on prevalence.

(Respondents could choose one option for each type of protection listed.)

Participants in the survey were asked a series of questions regarding their organization’s use of six different security technologies related to identity and access management (I&AM). These technologies enable an enterprise to establish identities for online users and validate those identities before granting access to sensitive resources such as networks, servers, databases and applications.

Prevalence of Security Measures

	Used universally	Significant use	Used moderately	Very little use	Not used at all
Password protection	60%	32%	7%	1%	0%
Two-factor authentication (tokens)	8%	19%	25%	17%	32%
Two-factor authentication (biometrics)	1%	3%	9%	22%	66%
Smart cards	4%	12%	11%	19%	54%
Web access management	16%	38%	27%	8%	11%
Encryption	11%	29%	41%	16%	3%

The methods referenced in the survey vary widely in their characteristics, including scalability, ease of deployment, total cost of ownership and risk mitigation. (See the sidebar “Beyond Password Protection” for a brief description of each method.) The survey questions were designed to elicit information on how widely these different methods are used today and how effective they are judged to be by CSOs.

Passwords Still Rule, But for How Long?

CSO responses, summarized in the table above, suggest that the majority of organizations use password protection as their “baseline” method for establishing online identities and authenticating users — and then selectively deploy other I&AM methods, based on the sensitivity of the application requiring protection and the cost/benefit equation for the organization.

The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

60% of security professionals said their organizations used passwords exclusively and 32% said they make “significant use” of passwords. By comparison, only 16% reported that their organization used web access management exclusively, 11% use encryption exclusively and 8% use two-factor token-based authentication exclusively.

From a historical perspective, the wide use of passwords is understandable. During the initial rapid growth of the Internet, passwords became the de facto standard for establishing and proving online identities. Password applications were inexpensive to deploy, easy to use and did not require end users to install any special hardware or software. In addition, automated tools have overcome some of the early inefficiencies of password administration, such as manual password resets.

However, over time, the shortcomings of password protection have become glaringly apparent — and increasingly difficult to justify. These shortcomings include:

- **Porous security.** For many reasons, some of them having to do with human nature, passwords are easy to hack, steal or guess. In fact, there is a veritable arsenal of high- and low-tech methods for stealing passwords. Newer techniques include “phishing” scams that use official-looking e-mail to lure users to phony web sites, where they are tricked into inputting passwords and other personal data.

There is also a new wave of keystroke loggers that can be installed remotely, without the system owner’s knowledge, and then operated covertly to capture passwords and other personal data. For all these reasons, passwords are an unreliable method for establishing and verifying identities

- **High costs.** The classic approach to password protection has resulted in each application having its own security system, which must be separately administered, managed and updated — with great duplication of effort. This is inefficient and costly for the enterprise and places a needless burden on overworked IT staff. In addition, users

I&AM — Beyond Password Protection

The survey asked CSOs to rate both the prevalence and the effectiveness of different technologies for identity and access management (I&AM). Alternatives to traditional password-based authentication and authorization schemes are briefly summarized below.

Two-factor Authentication — Tokens

Two-factor authentication provides a more robust proof of online identity than passwords and can be leveraged across multiple applications. This eliminates the need for an enterprise to support multiple security applications. It also eliminates the need for users to create and keep track of multiple passwords.

To gain access to sensitive resources, the user must present two identifiers or factors: something only the user knows — typically a PIN — and something only the user has. This latter factor is a token that displays a unique and frequently changing access code, which is generated by a secure and hard-to-compromise source.

Two-factor Authentication — Biometrics

This method operates on the same principle as token-based authentication. However, the second identifier is a biometric, such as a fingerprint or retinal scan — which some experts believe provides stronger proof of identity than token-based systems.

Smart Cards

Smart cards enable enterprises to consolidate employee badging and physical and network security onto a single device, thus reducing infrastructure costs while enhancing user convenience. One drawback is that smart cards require card readers at all access points, adding to the cost of deployment and maintenance.

Web access management

These solutions allow an enterprise to centrally manage user access privileges across diverse network resources and domains, again eliminating multiple security schemes. Organizations have fine-grained control over which users can access what resources. This approach also provides users with the convenience of single sign-on (SSO) across multiple applications.

Digital Certificates and Encryption

Many organizations require users to establish electronic credentials in the form of encrypted digital certificates, which cannot be easily intercepted or mimicked by a fraudster. Typically, the user must retrieve these credentials from a secure server and present them before being granted access to a protected resource.

Encryption is also widely used to protect sensitive data while it is at rest or in transit. Encryption makes data unintelligible to unauthorized users and extremely resistant to attack; it can only be decrypted by authorized users, who each hold a private “key” that is, itself, highly secure.

The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

managing upwards of ten passwords ultimately turn to IT for help. The resulting password-related help desk calls are staggering.

- **An unsatisfying user experience.** The proliferation of security systems leads to users having multiple identities and forces users to repeatedly traverse multiple applications. For users who spend much of their day accessing protected resources, navigating the intranet/extranet is much like driving in a city where there is a stop sign at every corner.

What Alternatives Are Being Used?

While passwords dominate, other authentication methods are clearly gaining traction. 70% of CSOs reported that their organizations make “significant” or “moderate” use of encryption; 65% make significant or moderate use of web access management; and 44% make significant or moderate use of token-based two-factor authentication.

Two technologies — smart cards and biometrics — are used far more sparingly than other methods. While smart cards have found acceptance in Europe and Japan, they have been slow to catch on in the U.S., where the survey was conducted. Only 27% of CSOs said their companies use smart cards moderately, significantly or universally, whereas 73% said they used smart cards very little or did not use them at all.

Biometrics are used even less frequently. 66% of security professionals said their companies did not use biometrics at all and 22% said they used them very little. Only 1% of CSOs reported that their companies used biometrics universally. This lack of penetration is likely due to two factors: the high cost of implementing biometric systems as compared to the costs of other authentication methods, and concerns about a “Big Brother” society that can track its citizens’ every move and choice.

X. Rate the following information security measures based on effectiveness.

It is an interesting exercise to compare the prevalence of various security methods with CSOs’ perceptions about the effectiveness of those methods. For example, while 60% of companies use passwords as their universal method for authenticating users, only 22% of CSOs said that passwords are a highly effective security method. It is reasonable to infer from this that, whenever the economics allow it — or the business need demands it — many CSOs will opt for an alternative approach that they view as being more secure than passwords.

So what other methods do they favor? Opinions are mixed. CSOs ranked encryption as the most effective, with 54% of respondents describing it as “highly effective” and 35% describing it as “fairly effective.” Token-based two-factor

authentication also received high grades, with nearly half of all respondents rating it as “highly effective” and 37% calling it “fairly effective.” Of these two technologies, encryption is currently more prevalent, with 11% of organizations using it exclusively and 29% making significant use of the technology. In comparison, only 8% of companies use token-based authentication exclusively and 19% use it significantly.

XI. Rate the following information security measures by their impact on the future of information security.

CSOs were asked to rate the future impact of five different security measures. Three of these have been previously defined — biometrics, smart cards and digital certificates, which are an application of encryption — and could be described as well established but still in various stages of evolution. Two of the choices — web services and identity management systems — represent emerging technologies.

The Web Services Challenge

Web services constitute the next evolution of distributed network computing. The web services model is based on the concept that highly automated, modular applications — each functioning as a discrete web service — will interact with each other, often without human intervention, to carry out complex business processes with a high degree of trust and assurance.

Implicit in this paradigm is the assumption that web services will be able to automatically and reliably vet the authenticity of other web services and of the people, devices and transactions that are encountered online. This requirement creates a new set of challenges in the realm of security technologies and has led to the development of web services standards for the secure exchange of identity information.

The Role of Identity Management Systems

In this new web services world, identity management systems will provide centralized capabilities for creating and administering online identities, reliably authenticating users and transactions, and managing access to protected resources (authorization) across the extended enterprise. While all these capabilities currently exist as “point” solutions, identity management systems will bring them together in a unified and highly automated environment that serves as an identity management authority.

The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

What Does the Future Hold?

Asked to rate the future impact of these technologies, CSOs gave answers that were distributed across a fairly narrow range, with those predicted to have a “high impact” or a “significant impact” as follows: identity management systems (75%), digital certificates (70%), biometrics (67%), smart cards (64%) and web services (64%). Further reflecting a similarity in viewpoints, only a small percentage of respondents thought that any of the technologies would have “no impact.” 1% said identity management systems and web services, respectively, would have no impact, 2% said smart cards would have no impact and 3% said biometrics would have none.

This parity may reflect strong opinions, deeply divided; it may reflect CSOs’ uncertainty about where technology is heading; or it may indicate that, with their different strengths, these diverse technologies will coexist for the foreseeable future.

RSA Security: A CSO’s Natural Ally

For CSOs confronting the security challenges discussed in these pages, RSA Security offers unmatched expertise and industry-leading solutions in two critical categories: identity and access management and encryption solutions.

By creating a more trustworthy and trusted e-business environment, these solutions enable organizations to confidently bring new business processes and service offerings online, thus increasing revenues, reducing costs and providing a more favorable total cost of ownership for security infrastructure

Identity and Access Management Solutions

RSA Security’s Identity and Access Management (I&AM) solutions enable organizations to create, manage, authenticate and authorize trusted identities, which can then be applied to any and all applications, data sources and transactions within the extended enterprise. Some of the key components of I&AM include:

Strong Authentication: Verifying identity

Many organizations now recognize that authentication — the ability to reliably verify user identities — must be the foundation for online services and business practices. Building on years of experience, RSA Security offers strong authentication solutions that help ensure the authenticity of people, devices and transactions.

- RSA SecurID® two-factor solutions employ hardware and software tokens to reliably establish the user’s authenticity, making it difficult for an impostor to masquerade as a legitimate user.
- One-time-use RSA® Mobile access codes are delivered to mobile devices, enabling enterprises to more securely extend popular web applications.
- RSA SecurID smart cards combine the functionality of physical and network access into one convenient, cost-effective device.
- The RSA Keon® family of digital certificate management solutions offer highly scalable authentication for legally binding electronic communications and transactions.

Access management: Controlling Who Has Access to What

RSA ClearTrust® software provides powerful, flexible capabilities for managing users’ access privileges, based on relationships (customer, employee, partner, etc.), roles (purchasing manager, HR specialist, software engineer, etc.) and specific attributes (account status, clearance, etc.). In addition to enhancing security, RSA ClearTrust software increases user convenience, enabling secure, single sign-on (SSO) across multiple applications and domains.

Digital Signatures: Authenticating Online Transactions and Communications

Digital signatures, which utilize digital certificate technology, are emerging as an effective method for authenticating online transactions and interactions. With RSA e-Sign technology, organizations can implement digital signature capabilities for online forms and e-mail, transforming these formats into trusted platforms for doing business.

Encryption: Protecting Data at Rest and in Motion

RSA Security database encryption solutions help to deter misdeeds by making the information in databases unintelligible to unauthorized users and extremely difficult to decipher when attacked. For example, even if a thief were to access a customer database, he would not be able to interpret the encrypted data — thus never ascertaining the real value of the information. RSA Security encryption solutions are also instrumental in protecting data that is in transit across networks.

The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions

A Vision for the Future

These RSA Security solutions have evolved from the company's long heritage in authentication, access management, administration and encryption. Building on this foundation, RSA Security offers a migration path to the identity management system of the future. Code-named NEXUS, this system will be engineered to integrate today's proven solutions onto a single platform that delivers a common set of services across all RSA Security enterprise products. The initial set of services will include:

- Identity authority services
- Access authority services
- User management services
- Provisioning services
- System services
- Network and application integration services

Components of NEXUS are already available in selected RSA Security solutions and will continue to be rolled out in future product releases.

A Commitment to Cross-industry Solutions

Complementing its focus on RSA Security enterprise products, the company is also working collaboratively to develop cross-industry solutions for identity management. As a founding member of the Liberty Alliance, RSA Security is helping to develop a global standard for federated network identity management. This approach will enable enterprises to securely share identity information while respecting the privacy wishes of consumers. Ultimately, users will benefit from the ability to navigate seamlessly and securely among protected e-business sites while businesses will benefit from the growth of revenues, reduced partnering and process costs and faster deployment of innovative new services.

In addition to the Liberty Alliance, RSA Security will remain a powerful voice in the public forums and standards bodies that address identity management and web services.

This commitment is evidenced by the company's continued involvement in OASIS and WS-I, which address the SAML and WS-Security standards and other emerging standards.

A Final Thought

CSOs face a daunting and ever-shifting set of threats and challenges. Yet, as this survey indicates, they are moving deliberately on numerous fronts to address these threats, deploying a combination of proven and evolving security technologies. In the realm of identity and access management, many enterprises are working with RSA Security to strengthen methods for maintaining user profiles, authenticating online users and managing user access privileges in heterogeneous e-business environments. The ultimate goal: to create a far-reaching e-business environment that is both trustworthy and trusted.

