Managing Secure eBusiness

An IDC White Paper sponsored by Novell

Analyst: Richard Robinson

IDC
Analyze the Future

Novell®

Introduction

The current mantra of business consultants is 'ebusiness or bust'. However, the stark reality is 'ebusiness security or bust'. Companies have always paid lip service to security, often claiming it is near the top of the list as a business priority, that is, until resources are to be committed. However, this must change. The explosion of internet commerce, forecasted to be worth $1.6 trillion by 2003, is offering organisations of every size opportunities previously unheard of. The potential customer base that the Internet provides is growing dramatically, from 327 million online users in 2000 to 600 million users in 2003 and the opportunities that this offers to individual businesses are massive.

The opening up of markets provided by the Internet is not only creating opportunities but also threats. At a revenue level, those organisations that do not take advantage of ebusiness will lose the battle to competitors both large and small, from near and far. But to truly take advantage of this new market environment organisations must open up their systems to unprecedented levels of users. However, with this comes significant security concerns. The negative effects on a business of having insufficient security systems in place or falling victim to security breaches and denial of service attacks are well recorded and have received numerous headlines during 2000. Although such situations should not be ignored, few organisations appreciate how having the correct levels of security in place can not only reduce the risk, but significantly enhance the opportunities which the Internet economy offers.

IT infrastructure security is no longer an issue simply confined to the IT department. The importance of security to business as a whole deserves the recognition and attention of senior management and the CEO. Security is not a 'nice to have' or 'insurance policy', it is becoming a critical foundation to business.

This White Paper, written by IDC, and commissioned by Novell, is the third in a series of papers which examines the development of business along a technology pathway, or as defined by IDC, the electronic business continuum. This paper aims to examine the area of security in the context of the development along the electronic business continuum, and illustrates how having the correct systems in place can positively impact an organisations' bottom line.

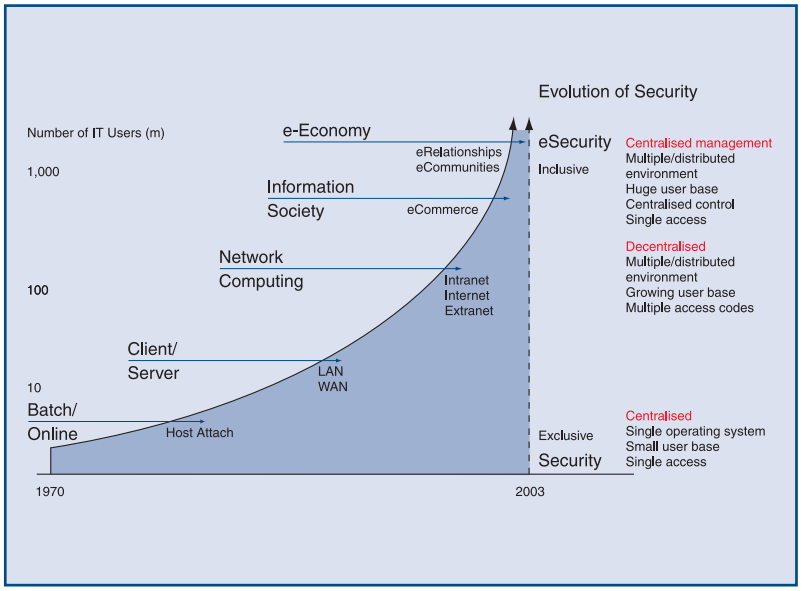
IDC's electronic business continuum

As outlined in the preceding White Papers, IDC believes that central to electronic business adoption is a change, a progression, along an organisations technology pathway. The basis of the idea is that organisation's business processes evolve along the electronic business continuum, where business processes develop in concert with technology advances. Business today has truly reached the stage where electronic business is at the heart of its processes.

The continuum is always evolving. As ebusiness develops IDC believes that the next phase will be based around electronic relationships and ecommunities where the relationship and the interaction between all communities is of critical importance. It is in this environment that a true e-economy will flourish. Figure 1 illustrates the continuum as an historical progression. Highlighted in the figure are the IT era; Batch/Online, Client/Server, Network Computing, the Information Society and the predicted next stage of the continuum, the e-economy. Also sign-posted along the continuum are the key prevailing technology milestones and the changing requirements and dynamics of security. How security has developed from an 'exclusive' to an 'inclusive' strategy.

Security in the first IT era, that of batch/online and mainframe computing, was relatively straightforward. Generally there was one operating system, with one access point, and users were few in number. We then experienced the IT era of client/server and network computing, where organisations developed decentralised IT infrastructures, with mulitple platforms and operating systems. This coincided with a dramatic increase in the number of users accessing these systems. This led to the installation of a multiplicity of security components, all of which required individual access codes and policies, which was a major impediment to the deployment of good security strategies and practices. As we enter the information society and move into a true e-economy it is apparent that organisations need to regain control of security. With the explosion of applications, systems and especially in the volume of users ebusiness will bring, rationalisation of security is essential. A return to centralisated access control and security will be the only effective and efficient way of managing this situation.

Figure 1
The Electronic Business Continuum: The Evolution of Security



Source: IDC, 2000

Until recently, security in a networked environment was just about 'keeping the bad guys out', it is now increasingly important to let the 'good guys in'.

IDC believes that the business environment is similar to an ecosystem, where a change to one element has a knock-on effect elsewhere in that ecosystem. Currently, the most profound effects being felt in the business ecosystem are caused by electronic business. eBusiness has had an impact on every aspect of the modern business model from IT infrastructure to channels to market. This is also true for security. Until recently, security in a networked environment was just about 'keeping the bad guys out'. However, as businesses move along the electronic business continuum towards the e-economy, where organisations are extending connectivity via extranets and the Internet, it is increasingly important to let the 'good guys in'.

So what do we mean by 'good guys?' The term 'good guys' really revolves around the concept of 'trusted relationships'.

As with traditional businesses, trust and a set of guiding policies are key. For example, a traditional retailer does not expect potential clients to be kept outside the shop window looking in with no way of accessing the goods. Customers are welcomed into the store to browse, become informed about the product and try it on for size

before deciding to make a purchase. This is all done with an element of trust; that the goods will not be damaged and that the customer will not steal from the till, or run out of the store without paying. Now, areas of that trust are backed up by security processes, for example alarms on the exits and access controls on the tills. These principles are the same when the business is transferred to an electronic based relationship.

However, in the e-economy these relationships can go much further and involve a greater number of organisations including partners, suppliers, employees as well as customers. All of these groups need to be given secure, controlled access to specific resources in order to facilitate business relationships.

As the role of security in the e-economy evolves, so must an organisation's security policies and procedures.

As the role of security in the e-economy evolves, so must an organisation's security policies and procedures. For example, the traditional perimeter defences of firewalls and smart routers that protect corporate assets from the outside are no longer enough in an age of opening accessibility. Organisations need to develop an esecurity policy around controlled managed access throughout a distributed environment. Those that do not develop specific esecurity policies, and rely on legacy procedures, will be unable to take full advantage of the opportunity that ebusiness offers.

In the past, attitudes to security have been based on the cost of installation offset against the likely negative cost implication of a security breach. However, as market dynamics change between an organisation, its partners, customers and employees, the business pressure to extend online access suggests that security actually enables new kinds of business process. eSecurity should be viewed as enabling business to grow and as a catalyst to increase revenue, it is about living in an era of accessibility, trusted relationships, open communication, certified information and proactive systems.

What is the impact of ebusiness security on my organisation?

Some organisations will not wish to develop along the electronic business continuum, and this is fine. Organisations that use IT in the back office only and are not connected with the outside world have a significantly lessened chance of suffering security breaches than those that are working in the e-economy. From one (very limited) perspective, a company could consider it wise to stay out of the e-economy in the interests of protecting its assets and resources while assuring customers of a secure business environment.

Organisations that choose to keep themselves out of the ebusiness arena will most certainly suffer at the hands of their connected competitors.

In reality, however, organisations cannot afford to stay within their castle walls. Even in environments that require optimal security, such as finance and healthcare, organisations are making themselves available to customers in any way that suits them — be it in person, over the phone or via the Web. This means organisations that choose to keep themselves out of the ebusiness arena will most certainly suffer at the hands of their connected competitors.

Security: Insurance policy or competitive advantage

Enlightened organisations are beginning to regard the security of their systems not as an insurance policy, but as a competitive advantage. IDC believes that this is the right approach if organisations are to take full advantage of the new market dynamics brought about by ebusiness. Organisations planning to compete in the new environment will have to use a wide variety of security technologies and processes to secure every layer of the system. By creating trusted business platforms, an organisation can maintain high degrees of flexibility and launch new initiatives very quickly, without being constrained by poor security.

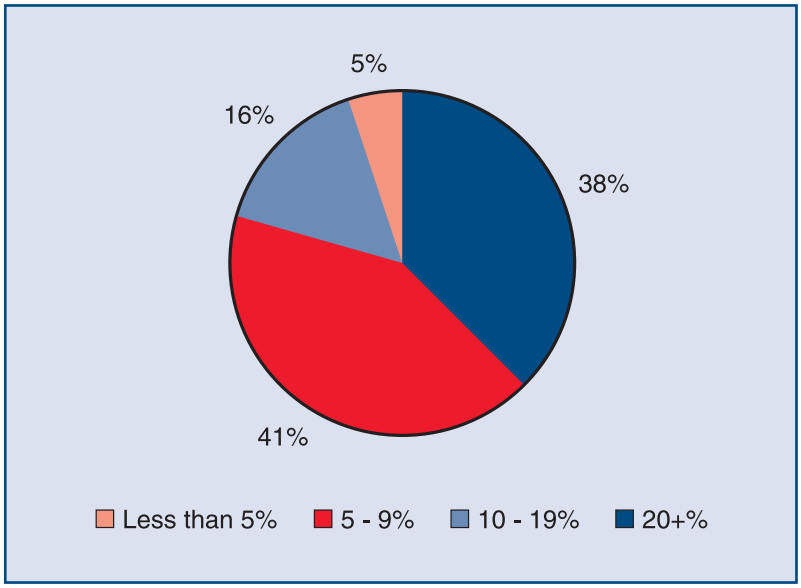
Once these platforms are built, trusted relationships can develop and then the true value of ecommerce can be realised.

The vast majority of businesses, however, still view security technologies and practices as insurance policies or worse yet, as inhibitors to growth. Once organisations realise the true value of an effective esecurity system, that is the value it can bring to an organisation in terms of revenue and shareholder value, the greater the likelihood of gaining the mindshare of senior management and, therefore, the funding that security deserves.

IT security spending

IDC research shows that spending on security varies greatly from organisation to organisation, but the majority is spending less than 10 percent of IT budget on security solutions. However, spending is beginning to increase as the business needs dictate. The research results show that 53 percent of the organisations surveyed plan to increase annual expenditure on security measures by an average of 5 percent of their IT budget in the next year.

Figure 2
Proportion of IT Budget Spent on IT Security



Source: IDC, 2000

Benefits of esecurity to business

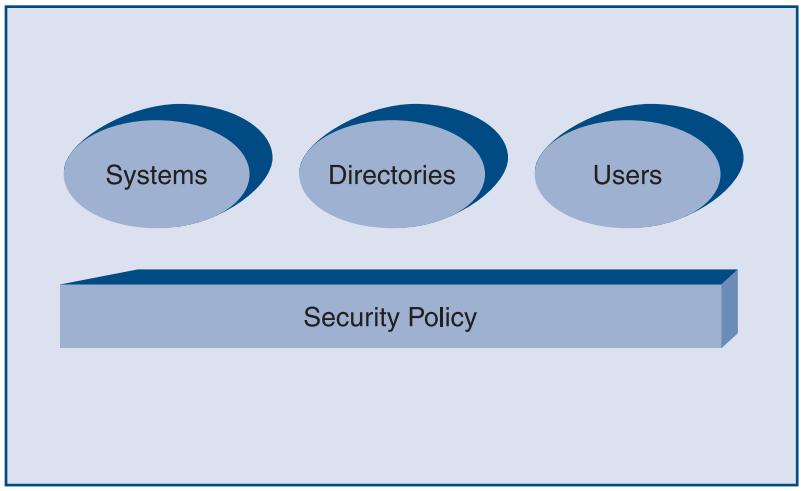
With the increase in networking of formerly disparate systems, via an Intranet, organisations need to ensure that employees gain the correct level of access to the right systems. As sensitive applications such as accounting, sales and HR are linked there is a greater need for implementing multi-factor user authentication, graded access control, and most importantly, a security audit. However, controlled access to systems will bring about 'knowledge workers' that can positively impact an organisation's business. Telephone banking offers a good example of how this concept can be best used. A customer telephones his/her bank to obtain an account balance, the customer service representative provides the requested information and the conversation finishes.

However, a customer service representative who not only has access to the customers account details, but knowledge of the business and its products is able to identify that the customer would benefit from a higher interest account or a different type of savings product. The customer service representative raises this fact with the customer and this can lead not only to the opportunity for an additional sale, but provide the customer with a value added service. The value of customisation or personalisation of customer interaction cannot be understated in an era of diminishing customer loyalty.

Centralised security system

The example above illustrates the potential for increased sales and improved customer loyalty, but how is this achieved? By having a centralised security system that allows controlled access, through authorisation and authentication for each user. However, creating, monitoring and amending such a centralised system is a daunting task when the multiplicity of systems, applications, operating environments, number of users, as well as integrating the complexity of security devices, is taken into account. The utilisation of a directory system can provide the backbone to an effective and efficient centralised security system. Through the use of a directory, security policies can be set and managed by one central administrator, no matter how decentralised an organisation is, how many platforms and operating systems are installed, or how quickly the user base grows. The figure below provides a simplified model of the functionality required:

Figure 3
A simplified model of security functionality

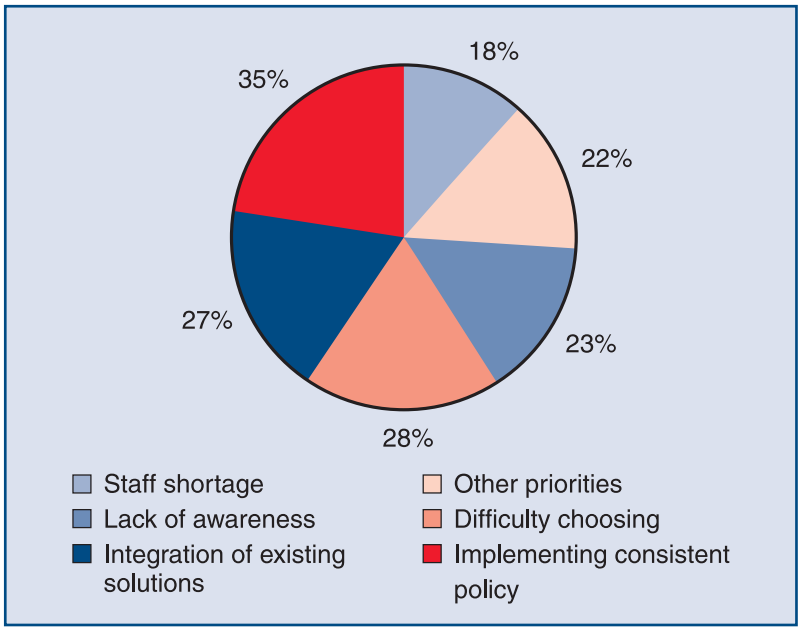


Source: IDC, 2000

The value in having a centralised security system can, in itself, also provide positive business benefits to an organisation. Implementing stringent password policies, diligent auditing systems, complex authorisation and authentication procedures and technologies, such as biometrics, can be time consuming and expensive. This can be alleviated by a centralised security system that offers a single point of administration, leading to a reduced number of individuals involved in setting up and running the system. Also commonality across security methods will reduce the costs associated with management and training.

These are important factors when one examines the obstacles faced by IT managers when implementing security. In a survey of IT managers, respondents stated that the primary obstacles to implementing security solutions were 'implementing consistent policies' and 'integration of existing solutions', issues that a centralised security strategy will alleviate.

Figure 4
Primary Obstacles to Implementing Security



Source: IDC, 2000

Allow the good guys in

When the systems are opened up to partners the level of access control is equally as important. eBusiness can significantly improve and streamline supply chain management. By allowing a supplier access to elements of an organisation's business that impacts upon that relationship, the supplier is able to better understand the organisation's business and improve its service accordingly. For example, allowing a supplier to understand the run rate of sales will provide them with the information to predict peaks and troughs, potentially reducing the need for warehousing/storage of goods, minimising such costs, and providing a more responsive service to the client.

A security policy must allow different users (partners, customers, employees) to have differing levels of access, based on defined criteria.

However, the varying level of trusted relationships that an organisation has with different partners requires differing levels of access. A 'one size fits all' approach to this access will limit the opportunities for business growth. A security policy must allow different users (partners, customers, employees) to have differing levels of access, based on defined criteria. However, the system has to be both flexible and scalable. This situation is at the heart of the power and opportunity of ebusiness, but is also the crux of the problem of establishing a secure system.

So what about the customer?

A major business benefit relates, strangely enough, to customer expectations. Both business to business and business to consumer customers are becoming increasingly IT savvy. These customers expect the organisations they conduct business with to provide a secure IT environment in which they can transact business.

Whether it is a contract for monitoring and managing an organisation's systems remotely, or an online purchase by credit card, consumers want to be reassured that their information is safe from fraudulent uses. As such customers are learning to expect more from their traditional providers of goods and services. Security will play an increasing role in customers' choice of provider as they realise the ease with which they can switch providers when they are dissatisfied with the level of service they receive. Customers will no longer be happy to stay with a provider that can not guarantee certain levels of security when another secure provider is a mouseclick away.

The importance of brand

Related to this is the matter of brand. As business increasingly moves from the "real" world into the virtual world of the Web, the value of a company's brand name will be one of its most important assets. In order to meet customers' expectations in cyberspace, organisations will have to ensure a secure ebusiness environment. Failure to do so will almost certainly result in depreciation of the organisation's brand and will directly impact the bottom line.

Reasons for investing in security

IDC research has identified that the key reasons for investing in security are firmly based on the business issues.

Figure 5
Reasons for Investing in Security

Source: IDC, 2000

As discussed throughout this White Paper, the opening up of an organisation's systems is fundamental to the development of ebusiness. As such, it is no surprise to see that increased network access is a leading driver for investment in security. What is interesting to see is that 'increased corporate awareness' is also leading the drivers. This is likely to be partly based on the coverage received in the media by a number of high profile security breaches.

To be able to implement security solutions it is vital that organisations' strategies take account of the flexibility and scalability needed to accommodate the cross platform and multi-application environment in which they operate.

These results also raise the important issue of organisations continually investing in new initiatives and new platforms. Organisations now operate in a cross platform and multi application environment. To be able to implement security solutions it is vital that organisations' strategies take account of the flexibility and scalability needed to accommodate this.

What can an effective esecurity policy achieve?

In summary, IDC believes that an effective esecurity policy can:

- Increase partner/customer loyalty – engender "trusted relationships"
- Improve supply chain and partnership management
- Increase system availability
- Empower partners and employees
- Manage change and knowledge management
- Reduce costs

eBusiness security strategy

IDC believes that security must be a consideration at every step of the development process of an ebusiness strategy. Best-practice security also demands regular attention to stay on top of the stream of new vulnerabilities that appear almost daily. Much of this process includes the use of security technologies, but a fair amount also includes making sure business processes and security policies are complementary. Perhaps the biggest problem with security is that it can appear to be too complex due to the fact that some level of security is required at every level of a system.

Organisations are going to have to realise that security needs to be an integral part of their business model.

However, technology is already driving security products towards becoming integrated, invisible and essential elements of an infrastructure. Organisations are going to have to realise that security needs to be an integral part of their business model.

A critical element for the success on an esecurity strategy is that a top down approach must be adopted. Security policies must be implemented and 'lived' at all levels of an organisation. IDC research has shown that the vast majority of security breaches occur from within an organisation, by employees being malicious or careless. The human factor can never be entirely controlled, however educating users, having features such as single sign on, and implementing an easily managed system, where users can be added and deleted quickly and efficiently, will all significantly reduce such occurrences.

The essential elements of esecurity

Key technology building blocks for secure ebusiness include:

- *Firewall*
- *Virtual Private Network*
- *Single Sign On*
- *Authentication & Authorisation*
- *Intruder Detection*
- *Virus Detection*
- *Secure Business Communication*
- *Certificate Management*
- *Network Control*

The essential elements of esecurity are:

- Trust: Assures the overall trust to facilitate ebusiness
- Non Repudiation: Precludes denial of a valid transaction
- Privacy: Protects data from unauthorised viewing
- Integrity: Protects data from corruption, destruction, or unauthorised changes
- Authentication: Verifies the identity of users, servers, devices and systems
- Encryption: Provides the underlying foundation for all esecurity components

In addition, systems availability should also be at the core of any security strategy. Availability is about systems, applications and data being up and running. There are many elements to achieving this, including, virus scanning, intrusion detection, audit and tracking, data and systems backup, and redundant hardware and software. The key is that when a system is down, it is not conducting business. A consequence of poor security policies is reduced availability.

User checklist

To ease the road to an effective ebusiness security system, IDC recommends organisations to follow these steps:

1. Have an independent ebusiness security assessment made. Leverage the experience and know how of other organisations
2. Have a specific ebusiness security policy in place
3. Be realistic – no one company can do everything – work with a company that is partnering with the top ebusiness security technologists – and – understands your business. A company that can offer a solution
4. Ask your chosen supplier for reference sites and case studies
5. Regularly revisit and update – ebusiness security should evolve with the business
6. Educate and train the users
7. Security is a board level issue and a top down approach is essential

Conclusions

Security, as with every other element of business, is being influenced by the evolution along the electronic business continuum. IDC strongly believes that organisations that integrate security considerations into the business process will have the ability to launch high-value applications faster and with greater confidence than ever before. Dealing with security in a tactical manner is no longer adequate and will not allow organisations to take advantage of ebusiness. Security is now a core business requirement, and security technologies enable an organisation to be a strong link in the ebusiness ecosystem.

Organisations that continue to regard security as a low priority or necessary evil, or even worse ignore it altogether, will not be well placed to succeed in this new business environment. In the end ebusiness security is not just about keeping the bad guys out, but also letting the good guys in.

Clearing a path through the security complexity?

The IT industry is proliferated with acronyms, buzz words and jargon, and the area of security is no exception. In fact, the area of security is a minefield of terminology through which organisations have to tread. The language, phrases and terms not only encircles the profession, but also excludes the masses. As such, some explanations are required.

Glossary of terms

Authentication

Verifying the identity of a user that is logging onto a computer system or verifying the integrity of a transmitted message. Authentication can be graded, according to an individual's need to access information, and can include more than one authentication procedure.

Biometrics: Means biological measurements and refers to eyes, voice, hand and fingerprints, which are used for authentication.

Smart card: A card with a built-in microprocessor and memory used for authentication.

Multi-factor authentication: The use of more than one authentication method, such as the use of a pass word and user name.

Graded authentication: Setting policies where individuals get different levels of access depending upon their requirements.

Single sign-on: A process that allows users to gain access to various/multiple systems and applications through the use of one authentication process, such as a password.

Cookie

Data created by a Web server that is stored on a user's computer. It provides a way for the Web site to keep track of a user's patterns and preferences and, with the cooperation of the Web browser, to store them on the user's own hard disk.

Session based cookies are based on the same principle but are deleted once the user disconnects from the Internet.

Cryptography (encryption)

The conversion of data into a secret code for transmission over a public network. The original text, or plain text, is converted into a coded equivalent called ciphertext via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end and turned back into plain text.

Symetric cryptography - The encryption algorithm uses a single key, which is a binary number that is typically from 40 to 128 bits in length. The data is "locked" for sending by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to "unlock" the code, restoring it to its original binary form.

Asymetric cryptography - A cryptographic method that uses a two-part key (code) that is made up of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt the messages, the recipients use their unpublished private keys known only to them.

DES (Data Encryption Standard)

A standard secret key cryptography method that uses a 56-bit key. It uses a block cipher method which breaks the text into 64-bit blocks before encrypting them.

The secret key may be kept a total secret and used over again or can be randomly generated for each session, in which case the new key is transmitted to the recipient using a public key cryptography method.

Triple DES

An enhancement to DES, applying 3 keys in succession, providing significantly more security than standard DES.

Digital signature

An electronic signature that cannot be forged. It is a computed digest of the text that is encrypted and sent with the text message. The recipient decrypts the signature and recomputes the digest from the received text. If the digests match, the message is authenticated and proved intact from the sender.

Signatures and certificates

A digital signature ensures that the document originated with the person signing it and that it was not tampered with after the signature was applied. However, the sender could still be an impersonator and not the person he or she claims to be. To verify that the message was indeed sent by the person claiming to send it requires a digital certificate (digital ID) which is issued by a certification authority.

Directory

A Directory Service is a database-based facility that enables administrators to manage all of the information in an enterprise, including user accounts, networking settings, connectivity, and operating system facilities. Directory services have been enchanced to scale to the Internet. These directories provide the foundation to grow and enable businesses to build and maintain secure and highly customised ebusiness relationships whilst leveraging existing technology investments.

Firewall

A method for keeping a network secure. It can be implemented in a single router that filters out unwanted packets, or it may use a combination of technologies in routers and hosts. Firewalls are widely used to give users access to the Internet in a secure fashion as well as to separate a company's public Web server from its internal network. They are also used to keep internal network segments secure.

Intrusion detection

Intrusion detection encompasses a number of techniques that seek to identify unauthorised access to systems discriminating them from normal system usage.

IPSec (Internet Protocol Security), ISAKMP (Internet Security Association and Key Management Protocol) and SKIP (Simple Key Management for Internet Protocol)

Open standard security protocols that provide authentication and encryption over the Internet. Used to enable secure VPN's to be implemented.

LDAP (Lightweight Directory Access Protocol)

An open protocol which allows applications to both get information from and put data to compliant directories.

PKI (Public Key Infrastructure) & Certificate Authority

PKI products consist of software products designed to register, issue, and manage the public and private keys related to digital certificates throughout the life cycle of the certificate.

SSL (Secure Sockets Layer)

An Internet security protocol. When an SSL session is started, the browser sends its public key to the server so that the server can securely send a secret key to the browser. The browser and server exchange data via secret key encryption during that session.

VPN (Virtual Private Network)

A private network that is configured within a public network or across the Internet. To maintain privacy in a public environment, VPNs use access control and encryption.

Virus

Software used to infect a computer. After the virus code is written, it is buried within an existing program. Once that program is executed, the virus code is activated and attaches copies of itself to other programs in the system. Infected programs copy the virus to other programs.

Corporate Headquarters
5 Speen Street
Framingham, MA 01701
508-872-8200

IDC Irvine
2171 Campus Drive, Suite 100
Irvine, CA 92612
714-250-1960

IDC Miami
Latin America Headquarters
5301 Blue Lagoon Drive
Suite 490, Miami, FL. 33126
305-267-2616

IDC New Jersey
120 Wood Ave South, Suite 509
Iselin, NJ 08830
732-632-9222

IDC Texas
100 Congress Ave, Suite 2000
Austin, TX 78701
512-469-6333

IDC West
2131 Landings Drive
Mountain View, CA 94043
650-691-0500

IDC Argentina
Trends Consulting
Lavalle 715 - Piso 7 B
CP 1047 Buenos Aires
Argentina
54-1-322-3159

IDC Asia/Pacific
Suite 2901-02, 29/F
Universal Trade Center
3 Arbuthnot Road, Central
Hong Kong
852-2530-3831

IDC Australia
Level 4, 76 Berry Street
North Sydney, NSW 2060
Australia
61-2-9922-5300

IDC Austria
c/o Loisel, Spiel, Zach Consulting
Mayerhofgasse 6, A-1040
Vienna, Austria
43-1-50-50-900

IDC Beijing
Suite A18, Yintai Office Bldg.
A-137, Xizhimen Wai Dajie
Beijing 100044, PRC
86-10-6833-1179

IDC Benelux
29 Avenue Louis Gribaumont
B-1150,Brussels, Belgium
32-2-779-46-04

IDC Brazil
Alameda Ribeirão Preto,
130 cj 41, 01331-000 São Paulo
SP Brazil
55-11-253-7869

IDC Canada
36 Toronto Street, Suite 950
Toronto, Ontario
Canada M5C2C5
416-369-0033

International Data Corp. Chile
Luis Thayer Ojeda 166 Piso 12
Providencia, Santiago 9
Chile
56-2-231-0111

IDC Colombia
Carrera 90 No. 156-19, Piso 5
Santafe de Bogota, Colombia
571-680-3100

IDC East Central Europe
Korenskeho 7
150 00 Praha 5
Czech Republic
420-2-544-073

IDC Egypt
39 Iraq Street
Mohandesseen, Cairo, Egypt
20-2-336-9379

IDC España
Ochandiano,6
Centro Empresarial El Plantio
28023 Madrid
+34-91-7080007

IDC Finland
John Stenbergin ranta 2
FIN-00530
Helsinki, Finland
358-9-7016377

IDC France
Immeuble La Fayette
2, Place des Vosges
Cedex 65
92051 Paris la Défense 5 France
33-1-49-04-8000

IDC Germany
Westerbachstr. 23A
61476 Kronberg/Ts.
Germany
49-6173-7098-0

IDC Hungary
Bajcsy-Zsilinszky út. 57
Building 3, Rooms 103-104
H-1065 Budapest, Hungary
36-1-153-0555/ext. 165, 166

IDC India
206, 207, Saraswati House
27, Nehru Place
New Delhi 110 019, India
91-1-6419754

IDC Israel
134 Rothschild Blvd.
Tel Aviv 65272, Israel
972-3-685-8093

IDC Italy
Viale Monza, 14
20127 Milano, Italy
39-02-284571

IDC Japan
10F The Itoyama Tower
3-7-18, Mita Minato-ku
Tokyo 108-0073, Japan
81-3-5440-3400

IDC Korea Ltd
13th Floor, Textile Center
944-31,Daechi-3Dong
Kangnam-Ku, Seoul, Korea
82-2-528-5100

IDC Malaysia
Suite 23.1 23rd Floor
Menara Genesis
33 Jalan Sultan Ismail
50250 Kuala Lumpur, Malaysia
60-3-244-3715

IDC Mexico
Select - IDC
Av. Nuevo Leon No. 54 Desp. 501
Col. Hipodromo, Condesa
C.P. 06100 Mexico, D.F.
525-256-1426

IDC Netherlands
A. Fokkerweg 1
1059 CM Amsterdam
The Netherlands
31-20-669-2721

IDC New Zealand
Level 4
43 High Street
Auckland, New Zealand
64-9-309-8252

IDC Nigeria
House 2, 'C' Close
403 Road, 4th Avenue
New Extension, Festac Town
Lagos, Nigeria
234-1-883585

IDC Poland/ProMarket
Wrobla 43
02-736 Warszawa, Poland
4822-644-4105

IDC Portugal
c/o Ponto de Convergencia S.A.
Rua Leopoldo de Almeida 4A
1750 Lisbon, Portugal
351-1-758 31 26

IDC Russia
c/o PX Post, RDS 186
Ulitsa Zorge 10
Moscow 125525
Russian Federation
7-501-929-9959

IDC Scandinavia
Jagtvej 169B
DK-2100 Copenhagen
Denmark
39-162222

IDC Singapore
72 Bencoolen Street #02-01
Singapore 189643
65-226-0330

IDC South Africa
c/o BMI-TechKnowledge
3rd Floor, 356 Rivonia Blvd.
PO Box 4603
Rivonia, 2128, South Africa
27-11-803-6412

IDC Sweden
Box 1096 Kistagången 21
S-164 25 Kista, Sweden
46-8-751-0415

IDC Taiwan
8F-3, #547
Kuang Fu South Rd
Taipei, Taiwan, R.O.C.
886-2-2729-6040

IDC Thailand
27 Soi Charoen Nakorn 14
Charoen Nakorn Road
Klongtonsai, Klongsan Bangkok
10600, Thailand
662-439-4591-2

IDC Turkey
Tevfik Erdonmez Sok.
2/1 Gul Apt.
Kat 9D; 46 Esentepe
Istanbul, Turkey
90-212-275-0995

IDC U.K.
British Standard House
389 Chiswick High Road,
London W4 4AE
United Kingdom
44-20-8987-7100

IDC Venezuela
Trends Consultores
Av. Francisco de Miranda
Centro Perú, Torre A, Piso 9
Of. 91, Chacao 1060
Caracas, Venezuela
582-261-0352

IDC Government
3110 Fairview Park Drive
Suite 1100
Falls Church, VA 22042
703-876-5055