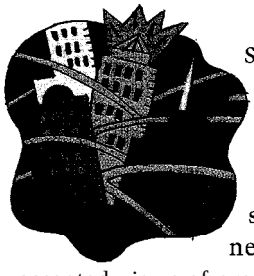
THE KEY TO Security

Without a consumer base that believes the Internet is a secure place to shop, electronic commerce won't flourish. Although many security companies say they can protect proprietary information and networks, as well as the privacy of consumers, users are still wary. In this article, Stephen Arnold, author of the recent book *Publishing* on the *Internet:* A New Medium for the New Millennium, dispels some of the mystery and myth surrounding on-line security, assesses its current state, and looks forward to new technologies.



SECURITY IS now recognized as one of the Internet's true weaknesses. In the seamless, global network, generally accepted views of protection, ownership and secure or private information are undergoing change. In many instances, traditional mechanisms of protection no longer function. The flows of data are too great and the resources needed for effective monitoring are not available. Nevertheless, people with assets want protection, or at least assurance that compensation will be paid and privacy maintained. The reality of the networked world is not congruent with these expectations.

The fears about security are real. On-line thieves steal more than $10 billion worth of data in the U.S. annually. A French student broke Mountain View, Calif.-based Netscape Communications Corp.'s security system for credit card transactions. America Online Inc., Vienna, Va., and Microsoft Corp. have both been plagued by a new type of security threat. Hackers created a Microsoft Word-delivered "mail bomb"-a simple electronic message that, when opened on the recipient's computer, destroys the contents of the hard drive. The result is loss of data. With mail on the most popular electronic information services expected to exceed one trillion messages a year by 1997, these security threats are an unpleasant development in the network medium. If one is not safe reading one's own mail, how safe are financial transactions, personal medical reports and other types of sensitive information?

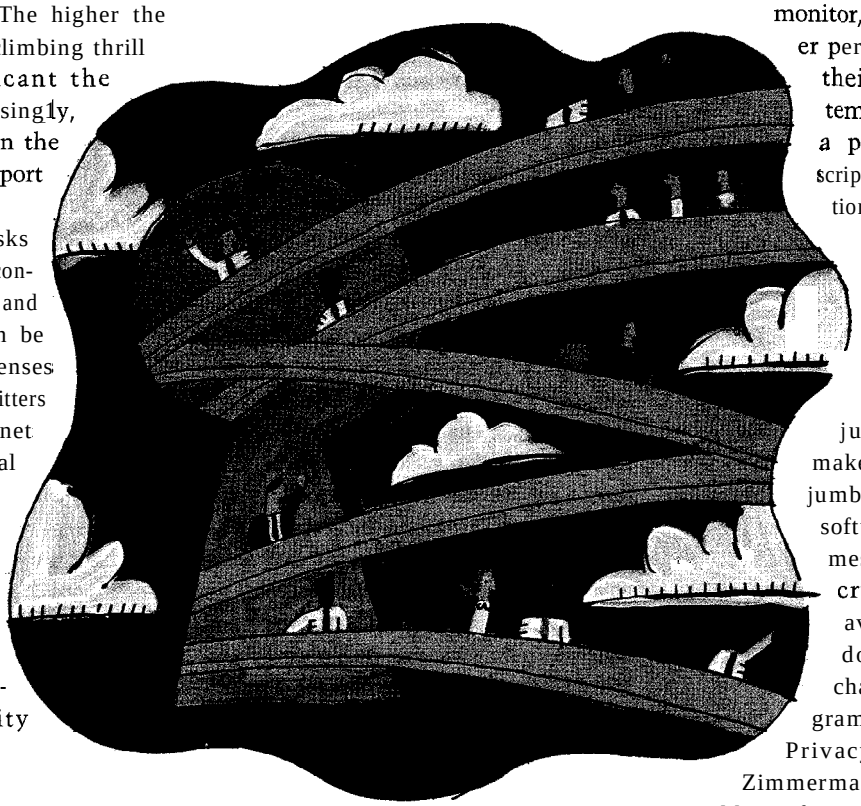
In the film "Hackers," Hollywood exploits the vulnerability of networks to experts with a chip on their shoulder—

BY STEPHEN E. ARNOLD

and in their laptop. What did not appear in ads for the film was the revelation that real-life hackers vandalized the Web site set up to promote the film.

If the present trend toward digitization and Internet linkage to data repositories continues, security will remain a pivotal subject for many years. Something akin to a tornado is taking place. More users, more information, more knowledge of systems and more payoff for high-value information all add up to greater security risks. As soon as one new feature is implemented, a clever programmer will defeat it. The rationale is similar to that in mountain climbing: The higher the barrier, the greater the climbing thrill and the more significant the achievement. Not surprisingly, the most hacked sites in the world are those that purport to have the best security.

With other media, risks were always present but controllable. Printing presses and photocopy machines can be locked up. Broadcast licenses can be revoked or transmitters disabled. But the Internet does not lend itself to local or even national controls. The technology and the social fabric of the global Internet community are in the process of redefining such concepts as copyright and privacy-and even security itself.



SECURITY BASICS

The first line of defense for a secure system is deciding what to protect and from whom. A security audit can identify information priorities. The individuals within the organization who have access to this information often provide the key to unlock the most elaborate systems. Security is only as good as its weakest link. If that link is a person within an organization, steps must be taken to ensure that the right people are on the job. The primary resource for security information is the National Computer Security Association in Carlisle, Penn. (firewall@ncsa.com).

The options available range from common sense to elaborate setups worthy of a James Bond film. The common-sense steps are the first ones to consider and, truth be told, for many situations they will provide the first line of defense. An organization or person must define minimum standards for a "security envelope" and then implement procedures to deliver that level of security. The most readily available and widely used tools are firewalls; encryption; and physical devices, also known as "dongles," that plug into a user's PC.

A firewall is either software or a software/hardware combination that lets authorized users into or out of a system and keeps out all others. Most firewalls require that the organization define two parameters for each user who is to obtain access via the firewall. The software firewall limits access from the public connection to the protected information on the server. The entire server can be protected by the firewall, or certain files or services can be protected. To accomplish this, the firewall software must know who can gain access, what type of verification is required, and the information on the server to which a person with specific authorization can gain access.

A typical hardware/software system designed for Internet use is Mountain View, Calif.-based Sun Microsystems Inc.'s Netra product, which retails for about $6,000. Netra watches the data packets to make sure that they belong to an authorized user. Variations on the firewall theme abound. The commerce servers from Netscape and Open Market Inc., Cambridge, Mass., include firewall functions, along with state monitoring and password functions to protect the data on the server from unauthorized access. For the majority of cases, properly administered password protection is sufficient. Intrusions or incidents occur mainly because of human error. Some people tape their passwords to their computer monitor, or give them to another person who wants to use their system. Typical systems can be breached when a person copies log-on scripts from PCs or workstations left running.

Encryption, or "payload security," offers additional protection. In the simplest form of encryption, readable text is converted into a jumble of letters that makes no sense. When the jumble is processed with a software key, the original message is displayed. Encryption technology is available in the public domain for little or no charge. One excellent program is PGP (Pretty Good Privacy), written by Philip Zimmerman and available from Boulder Software Engineering, Boulder, Colo. Commercial encryption tools are available from numerous vendors. Most of the more robust implementations are based upon technology developed at Stanford and Harvard universities and commercialized by RSA Data Security Inc., Redwood City, Calif.

Encryption technology comes in varying degrees of security. The cracking of the Netscape Navigator encryption technology by a student in Europe was due to a less rigorous encryption technique. A relatively short key was used to secure the message. Longer keys, 128 bits or more, are used within the U.S., but the country's export laws prohibit the sale of the technology outside its borders. Data

encrypted with shorter keys can easily be cracked. The longer the key, the less likely the message will be unscrambled.

Encryption is becoming more widely deployed to protect business information. IBM Corp. has introduced the "crypto-envelope." The idea is to combine encryption with verification that the sender and the recipient are who they say they are. The verification process permits a publisher, for example, to send a document to a customer. The information, if intercepted, cannot be read without the proper decryption keys. Also emerging are layers or wrappers of encryptions. A hacker bores through one layer, only to find that one or more additional encryption layers must then be decoded. Encryption systems are available from such companies as Cylink Corp., Sunnyvale, Calif.; Isolation Systems, Toronto; Raptor Systems, Waltham, Mass.; and Connect Inc., Mountain View, Calif.

The major vendors of Internet commerce servers have developed systems that implement encryption and various other checks on the authenticity of the sender and receiver of a message. Netscape has developed the Secure Sockets Layer protocol, which provides the capability to keep the connection between buyer and server private. Netscape has worked to make its SSL protocol the standard by providing the details of the SSL to the Internet Engineering Task Force (IETF; see "Internet Infighting," UPSIDE, October 1995).

Confusing and incompatible security standards are becoming a thing of the past. Visa International and Mastercard have agreed to pursue a common technical standard, called Secure Electronic Transactions (SET), for safeguarding payment-card purchases made over open networks such as the Internet. This mutually endorsed standard ensures that consumers and merchants will not have to choose or incur the costs of having different methods of accepting payments over the Internet. Visa and Mastercard appear to have leamed the lesson implicit in the VHS/Beta wars and, more recently, in the compromise between competing CD-ROM technologies: Common standards are more likely to succeed, and if you stick with a private standard that's not selected, you lose.

The common denominator of the new card-purchase standard is encryption technology and layers of security. The new standard promises to be more secure than a traditional credit-card transaction.

The third major category of security techniques is devices-cards, plugs, cables or a combination of them that are attached to a computer. When the computer is equipped with such a device, encryption, access information and log-on procedures are transmitted to a specific server. When a computer operates without the device, access is denied.

Faced with these three fundamental security options, how do you decide which one to select? Ultimately, the choice will rest on such factors as the degree of security being sought and the budget available.

SECURITY PLANNING

One can never be too thin, too rich or too secure. A point of diminishing returns is reached when the cost of providing security outweighs the value of the information or the effort required to run an Internet server. When the stakes are high, can any effort be spared to provide a suitable level of security? What is needed? How much must one spend to have a secure publishing site on the network? Tough questions, indeed.

There are three keys to Internet security: knowledge; appropriate support in terms of money, staff and hardware and software infrastructure; and people, usually the most difficult to control. The following questions help when tailoring a security system to a situation:

- What is the purpose of the security system? Is this server designed to permit public access to the data on the server while protecting the server from intentional or accidental harm?
- What is the user's or customer's expectation of security? Do those visiting the site have a tolerance for security precautions? Will users provide passwords, or will users forget passwords and expect some type of on-demand customer support to assist them?
- What particular information or parts of the system must be the most secure? What parts of the system can be comparatively open to outside access?
- What are the physical safeguards that must be taken to provide a suitably secure environment for the customers, employees and visitors?
- What person or organization will be responsible for the security precautions taken? Is a staff member able to handle this responsibility? Should security monitoring and operation be delegated to a third-party contractor?

Answering these questions provides a baseline of information upon which to build an appropriate security system.

The other dimension of knowledge pertains to the options themselves. Security can be visualized as a ladder. In order to reach the highest rung or the most secure information, more steps must be taken. How does one differentiate between a security system based upon passwords and authentication, vs a system based upon passwords that change on a weekly cycle and require authentication as well as a digital signature? Making such distinctions is important because the cost differentials can be significant—and in some instances, sobering.

The best guarantees for secure on-line services can be categorized as follows:

- Create a system that is tailored to the specific needs of the user or the customer. Complex log-on procedures are often resisted as too cumbersome for the pace of work.
- Anonymity is a powerful security step, in which the presence of the server is known only to a specific customer group.
- Content can be a security feature. Certain types of information cannot easily be copied either because the volume is too great (e.g., digital image libraries) or too volatile (frequent updates make it more efficient for users to get the most recent material automatically).
- Monitoring is enabled. A system, regardless of levels and types of security imposed, must be watched. When an intrusion occurs, action can be taken, from shutting down the server to monitoring the packets of the intruder. The data in the packets indicate the intruder's location (in most instances).
- Design the system so that different types of information or levels of service are wrapped in different security layers. Marketing information might reside on a public server with little or no formal security beyond a form requesting visitors to provide their name, address and e-mail address. More secure information can require a password and an

SECURITY SNAPSHOT

The building blocks for protection of information use and reuse

TECHNIQUES	HOW IT WORKS	YARDSTICK FOR USE	QUALITATIVE SECURITY RATING
Authentication	A process that reads bits and exchanges information with another server to determine that the sender has sent a message, not a person posing as a sender.	Promising technology for financial transactions. Technology is nor widely known outside of security specialists and. therefore. seems to offer promise for financialtransactions.	Midlevel; possibly very high. Will require specialized software on the render's and receiver's computer. *Weakness:* may be subject to software that fools the authenticaringsystem.
Encryption	Messages are encoded and cannot be read without a key. Fees for encryption technology range from zero for public-domain tools like Pretty Good Privacy to five-figure licensing fees for commercial-grade algorithms and support tools.	All public network traffic intended for a single reader should be encrypted.	Mid- to high-level security. Depends upon the type of encryption technology employed and the individuals who use that technology. *Weakness:* Decryption keys are cracked by hackers or leaked by a trusted user.
Firewalls	Software looks at each packet to make certain that the sender has authorization to use certain server-facilitated information or services.	All servers connected to the Internet should use firewall technology between the server and the Internet. If the server is connected to another network, another firewall is required.	Midlevel security. Proven technology. Many sources for both hardware, software and firmware implementations. *Weakness:* system administration faulty.
Password	Authorized users must enter a string of alphanumeric characters to gain access.	Password control is provided by most server software packages. Specialized password software is available to supplement the built-in functionality.	Low to medium level of security. Depends upon the user community, the frequency with whichpasswords change. and ocher security procedures.
Private Network	A value-added network reseller such as General Electric Information Services Co. Fees vary from a low of five figures to six figures or higher.	Techniques used by major banks and certain government agencies. Traffic runs on a proprietary network architecture or TCP/IP. Cost is not a barrier.	Highest possible level of security because it can implement all of the other techniques. Security can be compromised by a trusted individual. *Weakness:* A person can compromise the network.
"Hidden" Server	Users do not know the address for the server.	Early public systems available via dial-up from value-added networks offered little security. Once the server is located it can be hacked unless other security measures are taken.	Low to medium level of security. Depends upon the user community, the content and the other security devices in place.
Tokens	Special sequences of bits are embedded in the encrypted message. Special software adds data to a message or a file that provides information about origin, whether copies can be made, etc.	Promising technology to meter the reuse of certain types of information. Technology is nor widely known outside of security specialists and, therefore. seems to offer promise for publishers.	Midlevel;possibly very high if the embedded bits can resist tampering or being defeated by some type of spoofing technique. Weakness: not subjected to widespread public use. Vulnerability not known.

authentication process that is changed regularly.

. Make use of Web servers that are separate from mission-critical networks. The outbound Internet link is through a separate communications mechanism; for example, ISDN through the modem pool that supports transient connections. The public Web server is updated with a temporary connection to the organization's internal network.

. Use firewall and Web server software that support encryption and secure transactions. Supplement these steps with site-monitoring processes.

. Have security as a priority. Staff and a budget are required to maintain a secure environment. The most vulnerable sites are those with security procedures that are not maintained rigorously.

THE FUTURE OF SECURITY

The authentication scheme used by the original HyperText Transfer Protocol (HTTP) does not provide a secure method of user authentication or end-to-end protection across the Net. The body of an HTTP message is transmitted as clear text across the physical network used as the carrier. Consequently, anyone can masquerade as another person. The recipe for trouble compounds HTTP with such common ingredients as the open approach of Unix, the ethos of the Internet and the intelligence embedded in the packets of data.

The development of standards is difficult because any firm or individual may propose one to the IETF. Owners of existing authentication standards, like Microsoft and Netscape, have a significant market advantage. Although the technical details of each approach vary, they all make use to some degree of a

combination of techniques.

Identification and authorization (I&A) provides a starting point for system designers. I&A operates at different levels of stringency, depending upon the specific implementation. A single-level identification requires that specific information be provided to the system. In some implementations, the required information changes daily.

The more robust applications require the use of an external device (dongle) and specific personal identification numbers. A numeric token is generated by the device. Access is possible only when the I&A system generates the code required to establish access. Systems using encryption or a time-based code use public-key and private-key mechanisms to control access to the host. Rockville, Md.-based Virtual Open Network Environment Corp. (VONE) uses smart cards, precoded data and a PIN (personal identification number) in its system. [Information about devices used for I&A security applications can be found at Security Dynamics Inc., http://www.sdti.com; Digital Pathways Inc., http://dp.com; Cylink Corp., http://cylink.com; and VONE, http://www.v-one.com.]

A "challenge-response" mechanism has been developed by Bell Laboratories and is being explored by Mosaic licensee Spyglass Inc. of Naperville, Ill. The client and server agree upon a value derived from a password or other token. It is the value that is transmitted on the network, not the password itself.

Authorization technology that is now widely available from server software vendors offers two basic techniques to protect a site: **1)** User-name/password-level access authorization. The security can be assigned as a single user per password, multiple users per password, or group access per password, and **2)** Rejection or acceptance of connections based on the Internet address of the client, with network protection based upon matching packet addresses to a list of authorized points of origin.

There are several levels at which authentication can work. The building blocks of a secure system make use of one or more of these components:

- Rule file that defines which directory trees are public or protected.
- Protection-setup file that spells out the authentication scheme; that is, the process to determine that a packet has not been tampered with.
- Access control specifies the users, groups or domain names that have access rights for a specific directory.
- Password file that contains user names and passwords. This file can be automatically maintained by a tool that is provided with the server software.
- Group file that lists which user names and Internet addresses belong to which groups.

This array of I&A applications—including external devices, PIN numbers, challenge-response mechanisms and authorization technology-will surely grow in the future as Internet traffic and the threat of security violations command increased attention. Another development seems equally certain: Solutions to the Internet's security problems will be inextricably intertwined with privacy and copyright issues.

THE UNBREAKABLE LINKAGE

Most analysts of the Internet do not see the linkages that exist among the three issues of security, copyright and privacy, but the new medium requires a different way of thinking about each of these hitherto separate concepts. Security is more a matter of system design, planning and skillful technological implementation than an absolute. Publicly available networks are difficult to bend to the strictures of one-to-one confidential interaction. Regardless of the steps one takes, it is inevitable that someone will breach the system. Thus, the best remedies are planning, monitoring and appropriate staffing and resources.

Copyright laws in their present form are not up to the task of controlling the digital environment. Thus, the use of proprietary file formats, digital signatures, tokens and elaborate security procedures are effective-to a point. Then they break down, because virtually any type of digital information can be instantly copied, modified and moved from point to point in a matter of seconds.

Privacy is becoming increasingly difficult to protect in the new medium. One solution is the use of what CompuServe used to refer to as "handles" and "avatars" on the Internet. These are artificial personae that mask the identity of the user. However, if the look-up table with the real name and the false identity are breached, the concept of anonymity breaks down. Data about personal and private matters are a subset of security.

What is the outlook for these three issues? Are these problems substantive, or are they the fallout from the supernova of the Internet's explosion into popular consciousness?

First, these issues are real and vital. Internet technology has created an environment filled with paradoxes and contradictions. The medium's very openness is vulnerable because it is difficult to provide certain safeguards. After centuries of print, it should be possible to protect one's intellectual effort from inappropriate or unlawful use. Common sense might argue that such safeguards must be put in place; the reality of the new medium is that reasonable assurances are indeed possible. Absolute guarantees will be a long time coming, if they do come.

Second, creators and organizations have difficulty seeing that security, copyright and privacy are not separate issues. The long-term success of the new medium as more than a public-relations and marketing tactic hinges upon how we come to terms with:

- Providing access to the right person at the appropriate time to public, private, proprietary or confidential information.
- Implementing systems that provide appropriate safeguards that are neither onerous, costly nor ineffective.
- Managing the information about users of systems in some appropriate way so that abuses can be minimized.
- Building systems and processes that operate globally.

At this time, none of these four points has been satisfactorily resolved.

Third, solutions will not emerge from outside the new medium. The medium itself will have to generate solutions from within. Copyright is a consequence of the experiences of publishers, artists and other creators over centuries. The resulting body of law, despite its flaws, represents cumulative historical experience. The new medium has a short history. Furthermore, its dynamics make historical accumulation of experience almost laughable. Law and real-time quantum

changes in technical functionality have different time scales. Monitoring of new media activity is technically impossible. Regulation for most of the new medium's short history has come from the users themselves. Will the user community be able to generate solutions to the issues of security / copyright / privacy?

A solution or cluster of solutions will emerge over time. In the interim, the best safeguards are those driven by the careful design, implementation and monitoring of the information constructs created for the new medium.

NEW MEDIUM, NEW RULES?

Consider this: How easy is it for a dishonest person to work as a waiter for a day or two, copy the credit card number and expiration date of a well-heeled patron and use those numbers? Credit card companies struggle to contain such routine credit card theft. Cyberspace presents another class of problem entirely.

Cyberspace is new and not well understood by the majority of the world's population. Only 2 or 3 percent of the U.S. population uses on-line services.

Security hinges upon technology. The expertise required to design, set up, maintain and defeat various safeguards is outside the mainstream of most computer specialists. Security and threats to security are a form of war game. Each advance challenges those who would crack the system to renew their efforts to defeat the new barrier. Each breach leads to new safeguards. The cycle of measure and countermeasure is locked in a high-stakes game of one-upmanship.

Standards have not emerged because the free market promises huge financial rewards and significant competitive advantage to the organization able to impose its solution upon the Wild West of the datasphere.

National security agencies do not want security to prevent government monitoring of certain activities. Thus, secure systems are, in truth, not very secure. If they were, powerful entities of major governments would be blinded; that is, unable to "see" or monitor potentially threatening activities.

Unlike print or television, people in cyberspace are coalescing into a global market of sorts. Furthermore, there remain some vestiges of the climate of cooperation that characterized the pre-commercialization of the Internet. Crime in cyberspace is abstract and involves bits and bytes, not life and limb. An injured party might not know of an intrusion for years, or until an unexpected charge appears on a Visa statement.

But the tangible consequences of security breaches can be serious. A stolen credit card or calling card number can be disseminated globally in seconds. Vital medical information might be corrupted, with potentially life-threatening consequences. Companies can lose their credit or credibility and fail.

However, special care must be taken to set up interactive services that walk a fine line between reasonable security and procedures that alienate honest customers, The nature of network environments is that breaches of security are usually the act of one person or a small group of individuals working as a team.

But as the financial stakes grow, the payoff for wrongdoers will escalate. Security must respond, or the momentum of network publishing will be lost. Security will be one of the major business

opportunities during the next 12 to 36 months. Important trends that are gaining momentum include:

- Embedded, standard security. Major operating systems such as those from Sun, Novell Inc. and Microsoft's Windows NT include more robust tools.
- New hardware devices. The range of devices available for on-line interactivity is remarkable. Consider modems: laptop users must place calls through modems that provide the proper response.
- Firmware that provides user-defined security features. The AT&T/BBN Corp. Internet monitoring service incorporates proprietary software and devices to monitor and neutralize unauthorized users. The devices can be installed at the client site and monitored from anywhere.
- Network security features that will become more robust. The value-added network is able to enforce end-to-end security built upon various encryption technologies. Users will be able to authenticate their documents with digital signatures. Documents will include digital date, time and permission "stamps."

Despite all this, it is unlikely that network publishing will enjoy the type of safeguards associated with more traditional media. A document available via network publishing technology can be copied perfectly an infinite number of times, distributed globally in seconds and manipulated easily, and often automatically, into a new revenue-generating, network-published document almost invisibly. Digital trails are difficult to trace.

The potential of network publishing is not likely to be realized unless creators (authors, publishers and aggregators) can be assured that suitable protection exists for their products and services; that the money they collect can be credited to their account and used like hard currency, bank transfers or plastic credit cards; and that their business and personal activities can be conducted without fear of eavesdropping or compromise.

There can be no clear line drawn between what have traditionally been thought of as the separate domains of security (protection of systems and information from unauthorized intrusion), copyright (protection from unauthorized use of an intellectual product] and privacy (protection of information about an individual's private affairs). In the borderless world of cyberspace, legal, political and legislative resolutions of these issues are daunting tasks.

The psychological and technical barriers to Internet security have been breached, creating demand for a range of security mechanisms now becoming available. Those who want to buy via the Internet or use it for ED1 (electronic data interchange) can be assured that an appropriate level of security is possible for a wide range of applications. Companies with a properly conceived and constructed Internet security system are able to participate in this ongoing, fundamental shift in the way people do business. The shift allows significant opportunities for cost reduction, service innovation and competitive invention. In this wave of reengineering, the Internet emerges as a powerful, transformational medium. The issue is not whether the changes will come, but how soon. ■

Stephen E. Arnold is president of AIT, an information-engineering and technology-assessment consulting firm. *Publishing* on the Internet: A New *Medium* for the New *Millennium* is published by Infonortics Ltd.. London. Comments and queries may be sent to ssea@ntr.net.