Awareness and challenges of Internet security

Steve Hawkins
Technical Writer/Analyst, Dell Computers Co., Austin, Texas, USA
David C. Yen
Department of Decision Sciences and MIS, Miami University, Oxford, Ohio, USA
David C. Chou
Department of Business Computer Information Systems, St Cloud State University, St Cloud, Minnesota, USA

Keywords
Internet, Security, Computer networks, Companies

Abstract
Internet security is an important issue today. Corporate data are at risk when they are exposed to the Internet. Current technologies provide a number of ways to secure data transmission and storage, including encryption, firewalls, and private networks. This article discusses the awareness of Internet security and challenges faced in both the public and the private sectors.

Introduction

The threat of computer security is one of the main barriers to Internet commerce. With the current popularity and the potential profits of e-commerce, many executives face a conflict situation. That is, connecting to the Internet and expanding their business would risk the threat of intrusion. On the other hand, remaining disconnected from the Internet would sacrifice their customer contact and services.

Seven members of the Lopht Heavy Industries, an independent watchdog group composed of seven hackers, informed the Senate Committee on Governmental Affairs in 1998, that "it would take only 30 minutes for them to render the Internet unusable for the entire nation" (Yasin, 1998). There is more. Officials from the General Accounting Office (GAO) also met with the committee and stated that the GAO has uncovered serious computer security weaknesses at both the State Department and the Federal Aviation Administration that could jeopardize the operations of both governmental agencies (Yasin, 1998).

Organizations in both the public and the private sectors are aware of the needs of Internet security. It is interesting to know how both sectors take action to protect their Internet data and corporate systems. Internet security is recognized as the methods used by an organization to protect its corporate network from intrusion.

The best way to keep an intruder from entering the network is to provide a security wall between the intruder and the corporate network. Since the intruders enter the network through a software program (such as a virus, trojan horse, or worm) or a direct connection, firewalls, data encryption, and user authentication can restrain a hacker.

While many tactics provide assurance of protection, carelessness can also be a key factor. As a result, awareness training and education should be used to remind staff that an Internet security breach could have a profound effect on the health of the organization and, hence, their job security (Everett, 1998).

When a company is connected to the Internet, any user in cyberspace can have access to its Web site. Installing firewalls, intrusion detection systems (IDS), and user authentication software are the necessary precautions a company must take to protect themselves. Ultimately, the best protection from intrusion is to constantly keep watching for intrusion and to employ the best protection you can afford while travelling through the untamed terrain of cyberspace.

This article begins with an overview of Internet security and the technologies used in protecting the data on a computer system. Next, this article investigates the awareness of Internet security in selected industries from the public and the private sectors. New developments and challenges regarding data protection and Internet security are addressed in the last sections.

Technology for Internet security

There are a variety of methods that a company can employ to protect itself from unauthorized access. Some of the most popular methods are:

- firewalls;
- user authentication;
- data encryption;
- key management;
- digital certificates;
- intrusion detection systems (IDS);
- virus detection;
- virtual private networks (VPN);
- extranets.

Information Management & Computer Security
8/3 [2000] 131–143

[ISSN 0968-5227]

Information Management & Computer Security
8/3 [2000] 131–143

Table I illustrates the unique features and the limitations of all of these Internet security methods.

Implications of security methods

Firewalls are the first line of defense for corporate networks. A firewall is a combination of hardware and software that separates a local area network (LAN) into two or more parts for security purposes. All public connections to and from the corporate network initially pass through a firewall, which acts as a gatekeeper to give access to valid requests and, in the end, block out all other requests and transmissions (Cantin, 1999). In addition, firewalls can be implemented between departments to allow certain users access to secure data.

Another line of defense is user authentication. Basically, a user must enter a password as a digital key to enter the computer system. User authentication can be incorporated into a firewall, a particular application, a document, or a network operating system such as Novell NetWare and Windows NT.

Table I
A comparison of Internet security components

Component	Unique features	Limitations
Firewall	Hides the corporate intranet from the Internet Acts as a gatekeeper to give access to valid requests, blocking out all other requests and transmissions Can be implemented between departments to provide certain users access to secured data Records all intrusion attempts for future review and identification	Software-only encryption may curtail firewall performance Presents a single point of failure No guarantee to protect a network from harm Must be installed and configured correctly in order to work properly
User authentication	Enforces user verification Can be incorporated within a firewall, application, document, or a network OS	User password could be intercepted during transmission User password could be related to their lifestyle, making password identification easier for hackers if they know the habits and interests of the user
Data encryption	Scrambles the data before transit, making interception attempts futile	Cryptology community believes that point to point tunnelling protocol (PPTP) technology may be flawed and unfixable
Key management	Acts as an electronic key to open encrypted data	User may lose the key or have it fall into the wrong hands
Digital certificate	Verifies the authenticity of the e-mail sender Alerts the e-mail recipient if the message has been altered	Not very useful if companies do not act as their own certificate authorities or get them from third-party service providers
Intrusion detection system	Uses static and dynamic methods to spot attacks to the network in progress or over time, respectively	No IDS product can detect all of the attacks on a network when it is heavily loaded IDS products work only on shared-access segments, and not on switched networks
Virus detection	Protects computers and servers from virus attacks	Useless if virus definitions are not updated on a regular basis
Virtual private network	An inexpensive way to connect remote users to an enterprise network Cheaper than using a dial-up connection	Some VPN products permit use of private addresses, while others require public IP addresses Flexibility may come at a price VPN product prices vary according to through-put and number of tunnels supported
Extranet	Provides fast data exchange between a company and its suppliers	Requires security and privacy systems to protect data during transmission

A user can incorporate a data encryption utility to protect the data while in transit. Basically, data encryption is a method of scrambling the data into an unreadable form before they leave a company's network. When the data arrive at the proper destination, a key decodes the data bits into understandable information.

There are basically three elements to an encryption system:

1 a method of changing the data into code (the algorithm);
2 a hidden place to start the algorithm (the key);
3 control of the key (key management).

A binary number usually provides the starting key for the algorithm. Transforming the data into a readable format is controlled by the key (DeVeau, 1999).

Key management, therefore, becomes an important factor in data security. The key must be secured in a safe place so those unauthorized individuals cannot access it. In most organizations, a system policy is developed that spells out who has the keys (and/or the power) to access sensitive data on the network (DeVeau, 1999).

Digital certificate is an electronic credit card that establishes the credentials for doing business or other transactions on the Web. A governing party called "certification authority" issues the certificate. This certificate contains the user's name, a serial number, expiration dates, a copy of the certificate holder's public key, and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real (DeVeau, 1999). Authenticated users keep these digital certificates in registries for access.

Digital certificates are similar to watermarks on a bank check. They not only verify that the author of the message is the author, but also alert the receiver if the message has been altered while in transit. Digital certificates are useful if the receiving party absolutely needs to know that the message they received is authentic (McCune, 1998).

To protect themselves from problems within the network, a company can use specialized software that monitors the network for suspect activity. The software not only detects intrusion from someone outside the company, but also monitors and detects any malicious activity on the network generated from the organization. This specialized software is called an intrusion detection system, or IDS.

Simply defined, an intrusion is someone attempting to break into or misuse the system. Intrusion detection systems, therefore, are a "trust no one" type of software monitoring system that spots attacks in progress, or over time. These systems can also reduce gigabytes of log entries into a graphical report that spots new trends on the network so management can spot intruders and stop them before they become a menace to the system (Giorgis *et al.,* 1999).

There are two types of IDS systems currently being used today: scanners and monitors. Both of these systems can be deployed on to a network or individual computers. Each system does a good job in detecting processes that are different from the norm.

Scanners are static IDS systems that basically sit and watch over a network system, like a security guard watching over a particular area of a building. IDS systems check for things like bad passwords, missing security patches, and misconfigured desktop computers. Some scanners will take a "snapshot" of the current state of the network, comparing it with a snapshot taken at a later date to see if there were any changes made in the system. If any changes in the system are unwarranted, this system could simply sound an alarm, or act proactively by replacing changed files with clean copies (Aviolo and Piscitello, 1999).

In contrast, monitors are dynamic systems that look for attacks to the network while in progress. Also known as threat monitors, they provide an answer to anomaly intrusions by monitoring the network and asking the question, "What is going on here? That doesn't seem right".

When evaluating an IDS, the network system administrator needs to make sure that the system addresses the following issues (Price, 1999):

- It must run continually without human supervision. However, it should not be a "black box" – that is, its internal workings should be examinable from the outside.
- It must be fault tolerant, that is, it must survive a system crash and does not need to have its knowledge base rebuilt at restart.
- The system can monitor itself to ensure that it has not been subverted.
- It must impose minimal overhead on the system.
- It must observe deviations from normal behavior.
- It must be easily tailored to the system in question. Every system has a different usage pattern, and the defense mechanism should adapt easily to these patterns.

- It must cope with changing system behavior over time as new applications are being added. The system profile will change over time, and the IDS must be able to adapt.

One of the worst threats on the Internet is computer virus. According to an *InformationWeek* survey, viruses "represent the single biggest computer and network security concern among businesses" (Larsen, 1999). Even with new, updated virus software in place, companies are still vulnerable.

Some industries use a virtual private network (VPN) to protect themselves from the outside attacks. A VPN is a private data network that uses public networks (such as the Internet), tunneling protocols, and security procedures to tunnel data from one network to another. A VPN is similar to a leased line. However, since the transmission vehicle is a public network, the overall cost is a lot less. The data sent along a VPN are usually encrypted before transmission and decrypted at the receiving end.

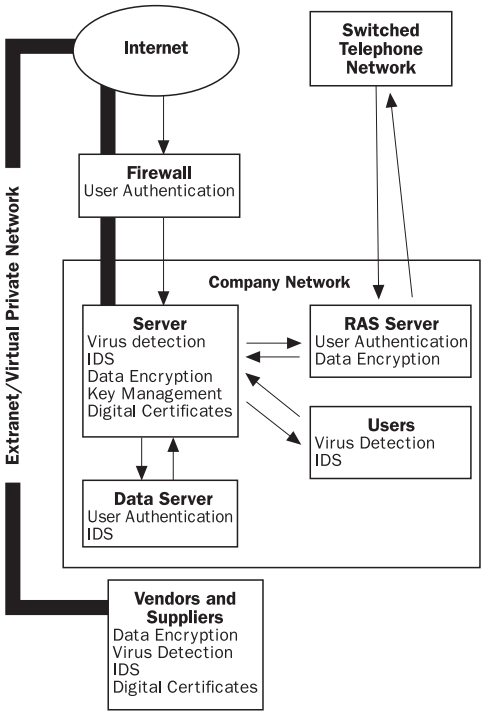
Another popular method of Internet security is extranet. An extranet is a private network that uses Internet protocols and the Internet to share a company's information with suppliers, vendors, partners, and customers. An extranet can be viewed as an extension of a company's Intranet that is shared with another related business. Companies that use extranets had previously large amounts of data exchanged with their suppliers using electronic data interchange (EDI).

Interoperability of security methods

All Internet security methods can work together within a network in various ways. As shown in Figure 1, user authentication is used to protect gateways from the outside, such as a firewall or remote access service (RAS) server. If a company wishes to protect sensitive data such as employee records, they can place these data on another server or computer that could only be accessed with the proper password. If a user tries to access this server and is not authorized to do so, the IDS will alert information technology (IT) staff of that entry, even though the user may or may not have the right password. Since the IDS use both static and dynamic monitoring systems to monitor direct attacks and abnormal network accesses, the server is dually protected from potential harm.

Data encryption is used throughout the network as well. Users calling in from a switched telephone network to a RAS server

Figure 1
Interoperability of security components



on a Windows NT network can use data encryption via point-to-point tunneling protocol (PPTP) to exchange data from their laptop or home computer to the Internet through the corporate network and vice versa. When a user is connected to the network through a RAS server, it is then giving this user the same access right as any other user in the company. The user can connect to the RAS server and send encrypted data to another computer or server using PPTP. The RAS server also has its own safeguards, such as user callback to a specific phone number to establish a connection and user authentication, encrypted passwords, and user permissions (Chellis and Donald, 1996).

Data encryption can be implemented between a corporate server and a vendor or supplier through an extranet. If data security is imperative on an extranet, both parties could encrypt the data to ensure privacy and data protection. Also, by incorporating a virtual private network on an extranet, both a company and its supplier can ensure maximum data protection on the Internet.

In addition to extranets and VPN, digital certificates and key management are two other alternatives for data security. If a company has an enterprise network that spans a large geographical area, corporate officials could use this technology to protect sensitive data from unauthorized access. For

example, if the human resources and finance departments need to share sensitive data, they could communicate through corporate intranet and use key management to protect the data and digital certificates to verify the accuracy of transmission. Even though VPNs and extranets provide some type of security, key management and digital certificates are simply two more locks and keys that could be set in place for peace of mind. Figure 1 shows the interoperability of Internet security methods.

Setting up a secured network is a daunting task. It requires careful thought, adequate planning, and the perspectives and recommendations of a team of IT staff. The network should be configured so that it is scalable and flexible to handle additional hardware and software as the network grows.

Hackers could breach several network devices, include the following (Abene *et al.,* 1999):

- *Domain name system server.* If properly configured, the server should only contain maps for hosts that must be known to the Internet community, such as DNS servers, external mail gateways, and the company's Web site. If the server is misconfigured, a hacker could perform port scans on servers outside the firewall and obtain user names and passwords to machines that were mentioned in the hosts file and were not listed in the DNS maps, thereby providing an access point to gain entry into the company's network.
- *Firewalls.* If not configured properly, a hacker could gain entry through machines located outside the firewall. Through an oversight or simply for convenience, a system administrator may open their firewalls to permit any type of network traffic coming in from these external machines.
- *Routers.* Most router vendors support password encryption, which would make hacker attacks more difficult. However, some administrators are either unaware of this feature or simply do not enable it.
- *Dial-up terminal servers with directly-connected modems.* These servers are often overlooked by system administrators or are managed by another group within the company with minimal communication between themselves and the administrator. Most organizations rely on dial-up connections, rather than the Internet, as part of their core business. They will not shut these servers down even in the event of an attack. This server is probably one of the most vulnerable servers on the network, since it is difficult to change the entire dial-up passwords and notify all of the users in a short amount of time. This will guarantee that the intruder will not be locked out of the network, if discovered.
- *Network administration server.* These machines typically run commercial network management software and often have trust relationships with other key servers on the network. They usually contain notes or comments about dial-up phone numbers for the dial-up terminal servers or, most importantly, contain boot images and configuration files for routers and terminal servers on the company's network. Since these configuration files usually contain unencrypted cleartext passwords for routers that are used for network boot clients, an intruder could use these passwords to gain access to other parts of the network.
- *Desktop PCs.* Some users may access their PCs from the outside, using software such as Symantec's pcANYWHERE. If this remote access software is not configured with a password, an intruder could access the hard drive on the PC and obtain sensitive data. In cases like this, users should be instructed to keep all of their valuable data on a company server in order to keep them safe from harm.
- *Mainframe computers.* Once an intruder is able to access this server, they usually can access just about anything on a company's network, making these servers the ultimate target.

As shown above, there are a number of areas in a company's network that are vulnerable to an intruder. The technology and hardware could be in place, but lack the proper configuration. This is why it is so important that IT personnel spend a lot of time thinking through their network architecture and ensuring that all of the bases are covered. Otherwise, the company could spend thousands of dollars on downtime, data loss, and backup from tape.

Table II lists the assessment of each data protection method.

Internet security awareness in the public sector

Government and educational institutions are the main players in the public sector. Similar to the private sector, the public sector receives equal pressure whenever they experience attacks from the Internet.

Government's awareness

Congress updated the Electronic Communications Privacy Act in 1986, which

Table II
Methods of data security

Method	Description
Firewalls	The first line of defense from the outside. Acts as a security guard for the company's internal network, filtering all incoming traffic from the Internet. A good tool for networks connected to the Internet
User authentication	Verifies the identity of the user. Could also be used to restrict access to certain resources within the network. A requirement for any user accessing a corporate network
Data encryption	Scrambles the data before and during transmission. Use this method when data protection is of importance
Key management	Acts like a "key" to access encrypted data. Maximum protection to protect data from unauthorized parties. Use this method in conjunction with data encryption to limit the number of eyes reading the encrypted file
Digital certificate	An electronic identification card that establishes your credentials when doing business on the Web. A digital certificate is similar to a watermark on a bank check. It verifies that the author of the messages is the author and informs you if the message has been tampered with while in transit. Use this method when proper identification is important
Intrusion detection systems (IDS)	Scans the network for abnormal activity, unauthorized resource access, and security breaches. Protects the network from both outside and inside accesses. A minimal requirement for any corporate network
Virus detection	Scans the network data for viruses, providing both prevention and cure if software is updated with the latest virus definitions on a regular basis. It is one of the best defenses for data protection. A minimal requirement for any corporate network
Virtual private networks (VPN)	A secure private data network that is developed on a public data network – like the Internet. Involves encrypting data before transmission and decrypting data on receipt. A good method to use for companies that wish to secure connections between two points on the Internet
Extranets	A secure private data network that uses a public data network – like the Internet – to extend a company's network to suppliers, vendors, partners, customers, or other businesses. It is the latest trend to share information with companies in the same industry. Use this method to minimize company overheads by exchanging data through an extranet via electronic data interchange (EDI)

was first enacted in 1984 as an anti-wiretapping act to combat the eavesdropping excesses of the Watergate scandal in the 1970s. Originally, the federal statute targeted telephone discussions without consenting those involved in the conversation. This act was updated in 1996 to include "all forms of digital communications, including transmissions of text and digitized images, in addition to voice communications on the phone" (AOL Legal Department, 1999).

To protect themselves from invasion, the Computer Fraud and Abuse Act was enacted by Congress in 1994. This act makes it illegal to access a federal interest computer. A federal interest computer which is known as a computer used by a financial institution, used by the United States Government, or one of two or more computers used in committing the offence, not all of which are located in the same state. Illegal activities may range from knowingly accessing a computer without authorization or exceeding authorized access to the transmission of a harmful component of a program, information, code, or command (AOL Legal Department, 1999).

As time moved on, the government has been instrumental in passing legislation to deter cybercrimes. In 1998, Robert Morris released a virus called a worm that crashed 6,000 computers on the Internet – roughly 10 percent of the computers on the Internet at the time – and was fined $10,000. As a result of his attack, and perhaps a last straw for action by the federal government, the feds initiated the computer emergency response team (CERT). Originally, CERT was an emergency response team and central point of contact for computer experts. Today, the work includes the following:

- help start other incident response teams;
- coordinate the efforts of teams when responding to large-scale incidents;
- provide training to incident response professionals;
- research the causes of security vulnerabilities, system security

Information Management & Computer Security
8/3 [2000] 131–143

improvement, and survivability of large-scale networks.

Currently, the CERT coordination center is located at the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University (Software Engineering Institute of Carnegie Mellon University, 1999).

To protect themselves from intruders, the federal government uses three levels of managing security, which, according to Campbell, need to be updated as technology changes. These are:

- establishing security policies and procedures and enforcing them, and
- implementing effective training programs for the lowest-level users through systems administrators, and refining network architectures and incorporating protection technologies (Peters, 1999).

While the Pentagon is investing more resources into network security, hackers continue to get more sophisticated. Still, the government continues to invest in countermeasures.

Educational institutions' awareness

Universities and colleges across the country adopt various types of security. At Miami University of Ohio, for example, many of the resources available to students must be accessed through a Novell NetWare server, which requires a log-on name and a password. When a student's log-on credentials are validated, he/she can access particular resources set up by the systems administrator. In most cases, this method is pretty secure, unless a student knows another student's birth date and social security number, which are both incorporated into the student's password.

Most colleges and universities apply a variety of safeguards on their network. System administrators can activate audit trails in their network operating system for monitoring abnormal file access on the network. For instance, on Windows NT, a systems administrator can set up an audit policy that tracks a variety of events, which include log-on/log-off, directory access, object access, and file access, to name a few. The systems administrator simply needs to monitor a log or set up alarms that warn him/her when certain files that should not be accessed by students are accessed. Using static IP addresses is another way of ensuring security on a network. Every network has a unique IP address that tells system administrators exactly where the computer is located.

Virus detection is another method that schools and universities use to protect their networks. In most cases, this is enough protection to circumvent any virus that may invade their computers. Most importantly, students should download new virus definitions each month from the school's network to their computers and update their anti-virus software. The school should also stress to students the importance of updating their virus definitions, as well as provide enough user education to show them how to update their anti-virus software on their own.

The Computer Security Administration Group at the University of Toronto, in Canada, is part of the Computing and Network Services group at the university. Their job is to develop and manage computer security programs for the university administrative computing systems and to provide consultative information security services to other areas of the university (Computing and Networking Services Department of the University of Toronto, 1999).

Some of their services to the students and to the university include:

- security awareness;
- security policy, procedures, and guidelines;
- disaster recovery planning support; and
- system monitoring and response.

By specializing in many different areas and having a disaster recovery plan set up in case of virus attack or disaster, the university will be best prepared for any problems that appear in their computer network.

Public sector's Internet security awareness

Both governments and educational institutions demonstrate their Internet security awareness by:

- employing the traditional methods of safeguards, which include firewalls, virus detection and IDSs, and user authentication;
- establishing security policies and procedures;
- informing their employees on the ethical use of the Internet and the consequences involved with its abuse;
- providing at least a minimal amount of training on how to use the organization's computer system;
- constantly monitoring networks for telltale signs of intrusion or virus attack;
- updating virus detection software regularly.

Information Management & Computer Security
8/3 [2000] 131–143

While these are all good tactics to use for most security problems, they are sometimes not enough. Considering the weaknesses associated in the public sector, there are always the issues of manpower and funding. Both the government and the colleges and universities across the country struggle with having enough resources to cover all of the bases and provide themselves with a strong front line of attack. Consequently, both parties are usually weak in the following areas:

- Accessing information from the private sector regarding network protection, computer viruses, and current industry protection methods.
- Developing an adequate ratio of manpower to protect the computer network that is in direct proportion with the amount of attacks experienced each day
- Providing adequate user education regarding safeguards in the use of floppy disks, e-mail, and homegrown software applications.
- Attending seminars and conventions related to the computer industry in order to stay abreast of current trends, problems, and innovations.
- Monitoring employees for any deviation in behavior on the organization's network and confronting any issues privately with these employees to ensure good relations and loyalty to the organization.
- Providing an adequate amount of protection to their computer systems that is proportionate to the value of the data stored on the system.

Internet security awareness in the private sector

The private sector consists of three main components, including finance, manufacturing, and service-based industries. All of these industries use similar methods to protect themselves, such as firewalls, virus detection, and IDSs. Each industry may use additional security methods.

Financial institutions' awareness

The financial industry consists of banks, brokerage houses, and any other companies that specialize in investments and securities. Financial institutions are currently providing their business services through the Internet. Current technologies such as secure socket layers (SSL), data encryption, and digital certificates provide decent protection to financial institutions.

While e-commerce provides a way to increase customer services and company profit, the level of security on the Internet is no near what is expected by the financial community. However, there are financial corporations who are finding ways to secure their networks.

One such company was Liberty Financial Cos. Inc. To provide better security for their customers, Liberty uses digital certificates to verify the identity of the customer and the authenticity of the site. As a result of their efforts, 15 to 20 percent of brokers and customers conduct e-commerce with Liberty using digital certificates, while other customers type in their names and passwords (Hann, 1999).

In most cases, companies that use the Internet to make cash transactions have installed SSL. Developed by Netscape, SSL is a protocol that encrypts data during transmission from a client to a server. Used heavily in e-commerce, SSL encrypts data in transit between the client and the server, but does not rescramble the data at the server site (Larsen, 1999).

While SSL has been a staple in e-commerce transactions, more sophisticated encryption methods, such as public key infrastructure (PKI) technology, are gaining momentum. This type of key management technology uses a string of numbers to encrypt documents from unauthorized access, and then decrypt them for authenticated users. Companies using PKI technology doubled from 6 percent in 1998 to 13 percent in 1999 (Hann, 1999).

Data protection methods, such as firewalls, data backup, and virus detection are also used quite heavily, with virus detection software at the top of the list. Since new viruses are discovered frequently, virus protection software is not always an effective way of protecting the system. Therefore, companies need to update their anti-virus software each month in order to protect themselves from damage.

Manufacturing industry's awareness

While the financial industry bases its security practices on encryption methods, the manufacturing sector uses a variety of alternate methods to secure their data. Even though some manufacturing industries use encryption for all of their documents, most of them tend to use secure connections called virtual private networks (VPNs) between their company and their suppliers.

A VPN is a method of simulating a private network over a public network. It incorporates tunneling, encryption, authentication, and access control

Information Management & Computer Security
8/3 [2000] 131–143

technologies and services used to carry traffic over the Internet. This definition varies, according to the vendor of this service. In essence, however, VPNs are not a single standard, but a set of tools (DeVeau, 1999).

Another type of private network that manufacturing incorporates between themselves and their suppliers are extranets. Somewhat similar to VPNs, extranets use a method of extending part of corporate intranet to another company to share business information or operations.

Extranets and VPNs can also be incorporated into one unit to strengthen Internet security. Since VPNs involve encrypting and decrypting the data before and after transmission, respectively, the extranet connection between both business partners is protected. A company could have multiple extranets connected to business partners and have VPN connections between a few of these partners for added security (Whatis.com Inc., 1999). Using extranets and VPNs together seems to be the best type of security for manufacturing, not only to protect themselves from outside invasion, but to further secure data from extranet partners who are not authorized to read the data.

Service industry's awareness

The service industry includes companies that are in business for themselves, providing some type of services or products for their customers. These companies include clothing stores, computer and software stores, etc. The service industry is one of the major players in e-commerce.

There are a variety of security methods that these companies incorporate to protect themselves from invasion. Most of them incorporate the traditional methods of security, such as firewalls, virus detection, and IDS. What is unique to the service industry is the goal of protecting the consumers, as well as themselves.

One of the primary methods of data protection is to have a secure connection between two parties. The most popular method of protection is SSL. When the user clicks on that button and the site has SSL capability, SSL is established between both computers.

While SSL is the current standard among e-commerce sites, it is not always the best. In May 1997, federal agents arrested a computer hacker who allegedly stole more than 100,000 credit card account numbers from an unnamed Internet service provider's (ISP) database. The hacker captured the credit card account numbers with the aid of "packet sniffer" software that scans data blocks for specific strings of information, such as credit card numbers. While the theft was itself a nightmare for both the consumer and ISP, what is also frightening is that the packet sniffer software is readily available on the Internet for anyone to download and use (Punch, 1998).

Private sector's Internet security awareness

In the private sector, the financial, manufacturing, and service-based industries have stronger data protection policies and practices that are different from their public sector counterparts. These include:

- virtual private networks and extranets that secure data transmission on a public network;
- stronger security between computers using technologies such as SSL;
- employing digital certificates to ensure the credentials of both the sending and receiving parties;
- data encryption for added security.

In most cases, the private sector differs from the public sector in providing additional security for the data, which includes verification and secure transmission and receiving. However, the private sector has its own set of weaknesses that provide loopholes in their safeguards. These include:

- The availability of packet sniffers that can circumvent security safeguards by intercepting data while in transmission.
- The currently outdated version of TCP/IP which provides little security for data transmission.
- The lack of establishing a 100 percent secure connection between the sender and the receiver.
- The lack of updated browser software on the user's computer.

New developments in Internet security

Each industry in both the public and private sectors uses similar security methods, but employ industry-specific precautions that are prevalent to their type of business. Each industry has its own particular needs, and requires certain safeguards to protect its data from damage.

Both the public and the private sectors have their own strengths and weaknesses on Internet security. Each industry requires certain safeguards to protect their data while in transit. Developing a plan that has proportionately more strength than weakness is always the goal. However, since

Information Management & Computer Security
8/3 [2000] 131–143

the Internet is still an untamed frontier that is still young and growing, it may take some time to develop stronger methods for data security.

Protecting an organization from the perils of the Internet is similar to the job of a security guard working during the night shift: as long as he stays awake and keeps his eyes open, the chances are that nothing will happen. While companies arm themselves with the latest IDS and virus software, there is still a chance that someone from the outside could get in and wreak havoc on the company's system. Software and hardware configurations keep most of the intruders at bay, but being able to recognize abnormal activity when it occurs seems to be the best method. This requires a well-trained IT staff who constantly monitor the network for deviants, using the system software to set up audits in all the right places. As technology continues to evolve and software and hardware improvements are implemented, there may come a time when hackers not only will be forced to stay outside the company walls, but also will be exposed by law enforcement during the process.

The future of Internet security, therefore, resides in human intervention and innovation. Implementing hardware and software solutions, as well as using human intervention to continually monitor the network, are two of the best ways to keep abreast of attacks from the outside. Fortunately, there are companies out there who see the need for high security and are working towards a better future for themselves and organizations alike. One of the latest technologies in the security market, that was introduced last year at the NetWorld + Interop trade show in Atlanta, is a new technology called adaptive security. This development is a result of Internet security systems' (ISS) formation of the adaptive network security alliance (ANSA) around an application program interface (API) for its real secure intrusion detection system (McClure and Scambray, 1998).

The technology requires the enlistment of major infrastructure vendors, such as 3Com, Lucent, Compaq, Entrust, and Checkpoint, to enable their products to talk with ISS's intrusion detection monitors. If ISS could enlist these manufacturers to incorporate a standard between themselves that will work in unison with ISS's detection monitors, unauthorized use of network resources will be difficult to accomplish. By developing better communication between ISS's monitor and the vendor's products, firewalls and switches could be reconfigured "on the fly" in response to perceived break-ins, thereby diminishing the lag time between detection and prevention and, ultimately, making the network virtually impossible to penetrate (McClure and Scambray, 1998).

In addition, SSL, the current standard for secure Internet transmissions used by credit card companies, may get a face-lift in the near future. To improve the security between themselves and their customers, the credit card companies have been developing another standard called the secure electronic transaction (SET) standard, which may have an affect on the security of Internet transactions. Basically, SET focuses on confidentiality and authentication. SET-compliant software will "not only make sure that thieves cannot steal a credit card number, but also keep a merchant from seeing the number while still providing assurances that the card is valid" (*PC Magazine*, 1999). The transmission will pass through the merchant's hands directly to the credit card user, which will then decrypt it and credit the merchant's account (*PC Magazine,* 1999).

Challenges for creating a better Internet security system

There are specific preparations that each company should do to protect themselves from the perils of the Internet. As every private business in town has its own individual requirements to keep itself in business, so does each organization in both the public and private sectors. Listed below are challenges that individual industries should take to develop a better Internet security system.

Government's challenges

- *Hiring IT professionals from the private sector.* It has only been a few years since the passage of the Information Technology Management Reform Act of 1996, which requires federal government officials to appoint CIOs within the walls of state and federal governments. By hiring IT staff from the private sector and providing them with a salary that is competitive with the market, government and state agencies can gain a wealth of experience from IT professionals (Couret, 1998).
- *Developing virtual private networks between state and/or federal departments.* The results of a 13-month security audit of the Federal Aviation Administration (FAA) concluded that Internet security is the lone area in which the State Department did not have adequate security (DiDio, 1998). By developing

VPNs between federal, state, and/or county offices, government agencies can "depublic" sensitive information from the Internet, thereby protecting themselves from Internet hackers and international computer terrorism (Communications News, 1998).

- *Providing research funding to private sector for developing Internet security technologies.* The federal government has suggested sharing information with the private sector. By providing research funding and/or tax credit, private sector companies may be more apt to work with governments.
- *Providing private sector training for government IT staff.* Since many of the innovations in IT are occurring in the private sector, government officials should ensure that their IT staff stays current by sending them to IT training. By staying alert to the innovations in the field, government agencies could steer themselves from tailing the leaders in IT to being a serious contender.

Educational institutions' challenges

- *Tailoring the classroom content to the needs of local industry.* It is important that professors and teachers in all levels of education receive current, real-world experiences in current IT technologies. One example would be developing relationships with industries near the school, thereby providing an outlet for new information in the industry which they can pass on to their students. By providing field trips to these companies and understanding their needs, graduates will stay current with IT technology and have a better chance of solving a company's IT security problems after graduation.
- *Recruiting educators in the private sector who have experience in the IT field.* IT companies may have well-educated employees who are aware of the problems associated with Internet security. By searching out these individuals who have experience in teaching, a college or university could gain a wealth of knowledge from these individuals, as well as provide students with knowledge and skills that companies desire in an IT college graduate.

Financial industry's challenges

- *Respecting the customer's right to privacy.* Companies that choose to sell their customers' personal information are actually hurting themselves. By developing a policy that gives the customer the choice as to how his/her personal information is disseminated, a company will gain more respect with their customers and eventually gather a large following of new business (Radcliff, 1999).
- *Using secure electronic transaction (SET) for maximum protection of customer financial data.* The current protocol used by most financial companies today is SSL. SSL has two problems:
  1. The merchant can read all of the data, which could end up in the wrong hands.
  2. Given sufficient time and energy, SSL transmissions can be decrypted by an intercepting third party.

  In SET, however, the data are forwarded by the merchant to an authorization center where they are decrypted, the purchase is authorized, and a receipt is sent back to the merchant, confirming the sale. Since the merchant never sees the customer data, it will ensure customer privacy. SET also has four advantages (Stamper, 1999):
  1. the data packets cannot be modified *en route*;
  2. only the transaction participants have knowledge of the transaction details;
  3. both parties are assured of each other's identity;
  4. the transaction is recorded; neither party can deny that the transaction took place.
- *Choosing an Internet service provider (ISP) that supports Internet privacy.* If a company decides to use an ISP for its Internet services, it should consider one that supports Internet privacy. In April 1999, 50 ISPs announced their intentions to support Internet privacy by joining Zero Knowledge Systems (ZKS) to form Freedom.Net, a consortium to provide users with untraceable pseudonyms that no one, including the ISP or ZKS itself, can track back to an actual person. By using one of these ISPs, companies could lessen the chance of transmitted financial data being intercepted by a third party (Zelnick, 1999).

Manufacturing industry's challenges

- *Employing a value added network (VAN) to support EDI communications.* VANs are companies which provide a variety of telecommunication services for their customers, have all of the equipment, software, and support already set up in their facilities. A company interested in EDI and not technically savvy could consider outsourcing this function to a VAN. VANs will handle all of the security

Information Management & Computer Security
8/3 [2000] 131–143

problems and overheads, allowing the company to focus on its own operations (Walsh, 1999).

- *Adopting a GroupWare application within a VPN.* Since the Internet is a public network, sending unsecured sensitive e-mail can be a dangerous maneuver. Instead, consider developing a VPN with a GroupWare application that connects both the company and its vendors and suppliers. If the company uses just-in-time (JIT) delivery, ensuring that the delivery of materials and parts on time is detrimental to company operations. Using a GroupWare application that maintains communications between both parties is a good way to ensure that all parties are talking to each other in synchronous time.

One of the latest GroupWare applications released by Lotus Development Corporation is Notes/Domino 5.0. This version supports "real-time access to relational data, transaction systems, and enterprise resource planning applications" (Biggs, 1999). The application also provides support for Java, JavaScript, and common object request broker architecture (CORBA), a new type of integration technology that works like a "software bus" to allow applications to communicate with one another, regardless of their design, platform, native language, and execution (Seetharaman, 1998).

Service industry's challenges

- *Using electronic funds transfer (EFT) to secure customer transactions.* Currently, there are only two popular ways to handle money on the Internet: credit cards and personal checks. However, there are other efficient methods to exchange funds on the Internet with less time.

  One type of Internet currency exchange is called electronic funds transfer (EFT). Here, buyers and sellers exchange digital money. Banks handle the transactions, but the customer authorization is made over the Internet. There are a few companies who have adopted this type of money exchange. Some of the major players are listed below:
  - DigiCash www.digicash.com
  - CyberCash www.cybercash.com
  - Mondex www.mondex.com
  - 1st Virtual Holdings www.fv.com
  - NetChex www.netchex.com
- *Employing specialized authentication systems to ensure a higher level of security.* One of the most popular methods of data security is using IDs and passwords to access a server or Internet site, but these are often inadequate. To address this problem, Axent Technologies has developed a hardware and software solution called Defender that creates unique, one-time passwords that cannot be guessed, shared, or cracked (Venetis, 1999).

  The system incorporates software on the user's computer that communicates with the Defender Security Server on the other end. When the user connects with the server, a software token is activated that automatically establishes a dialogue with the server. A new password is generated during each session, removing any possibility that the user will forget to change his/her password on a regular basis (Venetis, 1999).

Conclusion

As the Internet becomes the *de facto* platform for doing business today, it is still a vast frontier that is untamed and uncontrolled. Current Internet law protects "federal interest computers" from harm and makes Internet wiretapping a crime. But people continue to use the Internet as a means for their own gain, stealing the information and data from one company and making it their own.

One big dilemma with the Internet is that it is an invisible entity, viewed only through a small porthole called a computer. Criminals are in the form of ones and zeros – faceless people who disappear into the circuitry of a networked computer. Consequently, we rely on the small minority of computer gurus who produce the software and hardware that can "see" these intruders and stop them in their tracks. In most cases, these countermeasures work; in other cases, especially as technology continues to update itself and become more complex, the system fails.

It is important that corporate officials spend the time to educate themselves in IT. Fortunately, some companies have developed a new position of chief information officer (CIO). CIO ensures that IT operations parallel with the company's business plan and goals.

We need emerging technologies to protect privacy on the Internet. Depending on the type of business and the value of the data, a company has the choice of using virtual private networks, digital certificates, data encryption, and network operating systems to protect their data while in transit, ensure the identity of a user, and mask the data from unauthorized eyes. However, as technology continues to become more complex, the safeguards used today may be severely out of date tomorrow.

For this reason, corporate officials should require their IT staff to stay abreast of innovations and new trends in the IT field by attending seminars and subscribing to computer publications. Most importantly, corporate officials should make it a priority to sit in IT staff meetings, to read IT publications and to attend some of the training seminars.

References

Abene, M., Kovacich, G.L. and Lutz, S. (1999), "Intrusion detection provides a pound of prevention", at http: //www.network computing.com/815/815ws1.html

AOL Legal Department (1999), "Computer fraud and about act", at http://legal.web.aol.com/resources/legislation/comfraud.html

Aviolo, F.M. and Piscitello, D.M. (1999), "Intrusion detection joins net security arsenal", *InternetWorld*, March 22.

Biggs, M. (1999), "Workgroup and end-user software", *Infoworld*, Vol. 21 No. 7, February 15, p. 89.

Cantin, R. (1999), "Firewalls are the essential first line of defense," *Computing Canada*, Vol. 25 No. 3, January 22, p. 21.

Chellis, J. and Donald, L. (1996), *MCSE: NT Server 4 in the Enterprise Study Guide*, SYBEX, Inc., pp. 367-70.

Communications News (1998), "IP security for the tax man," *Communications News*, Vol. 35 No. 3, p. 66.

Computing and Networking Services Department of the University of Toronto (1999), "Computer security administration", at http://www.utoronto.ca/security/csaman.htm#CSAMAN

Couret, C. (1998), "CIOs perform high-tech juggling act", *The American City and County*, Vol. 113 No. 8, pp. 20-26.

DeVeau, P. (1999) "VPN = very profitable news", *America's Network*, Vol. 103 No. 8, May 15, pp. 36-8.

DiDio, L. (1998), "Federal agencies fail security test", *Computerworld*, Vol. 32 No. 21, May 25, p. 16.

Everett, J. (1998), "Internet security", *Employee Benefits Journal*, Vol. 23 No. 3, September, pp. 14-18.

Giorgis, T., Newman, D. and Yavari-Issalou, F. (1999) "Intrusion detection systems: suspicious finds", at http://www.data.com/lab_tests/intrusion.html

Hann, L.W. (1999), "E-commerce can create unexpected challenges", *Best's Review*, Vol. 99 No. 9, p. 75.

Larsen, A.K. (1999), "Global security survey: virus attack", *InformationWeek*, 12 July, pp. 42-56.

McClure, S. and Scambray, J. (1998), "Is adaptive security the next step in the evolution of a secure computing platform?", *InfoWorld*, Vol. 20 No. 44, November 2, p. 78.

McCune, J.C. (1998), "How safe are your data?", *Management Review*, Vol. 87 No. 9, pp. 17-21.

PC Magazine (1999), "The future of Internet security", http://www5.zdnet.com/pcmag/pctech/content/17/02/it1702.005.html

Peters, K.M. (1999), "Information insecurity", *Government Executive*, Vol. 31 No. 4, pp. 18-22.

Price, K. (1999), "Introduction to intrusion detection", at http://www.cs.purdue.edu/coast/intrusion-detection/introduction.html

Punch, L. (1998), "The real Internet security issue", *Credit Card Management*, Vol. 10 No. 9, pp. 65-7.

Radcliff, D. (1999), "A cry for privacy", *Computerworld*, Vol. 33 No. 20, May 17, pp. 46-7.

Seetharaman, K. (1998), "The CORBA connection", *Communications of the ACM*, Vol. 41 No. 10, p. 35.

Software Engineering Institute at Carnegie Mellon University (1999), "About the CERT/CC", at http://www.cert.org/nav/aboutcert.html

Stamper, D.A. (1999), *Business Data Communications*, Addison-Wesley Longman, Inc., Reading, MA.

Venetis, T. (1999), "Opening up for e-business doesn't have to be scary," *Computing Canada*, Vol. 25 No. 3, January 22, p. 19.

Walsh, B. (1999), "The nuts and bolts of business-to-business e-commerce", at http://www.nwc.com/904/904f2.html

Whatis.com Inc. (1999), "Virtual private network", at http://whatis.com/vpn.htm

Yasin, R. (1998), "Hackers: users, feds vulnerable", *InternetWeek*, May 25, p. PG1.

Zelnick, N. (1999), "50 ISPs to participate in new privacy network," *Internetworld*, April 26.