日本財団 The Nippon Foundation 助成

IIPS

Institute for
International Policy Studies
・Tokyo・

IIPS International Conference

"The IT Revolution and Security Challenges"

Tokyo

December 10-11, 2002

**"Open for Business but not Open to Attack –
Keeping Safe on the Information
Superhighway"**

by
Antóin Ó Lachtnáin
Chief Executive Officer,
Digital Messenger
Ireland

Open for Business but not Open to Attack – Keeping Safe on the Information Superhighway

IIPS, Tokyo – 11,12 December 2002

Digital Messenger Ltd.

http://www.digitalmessenger.biz/

22 Lr Grand Canal St
Dublin 2
Ireland

Antoin O Lachtnain
antoin@digitalmessenger.biz

Summary

The Internet and electronic communications are causing fundamental changes to the way businesses are structured. Although this brings many benefits, it also makes companies vulnerable to many new types of attacks. Because these attacks can be perpetrated over a long distance and can cause major disruption and damage, they are a serious issue for national security as well as for the managers of companies. There are many technical measures that can be used to help combat the risks, but these technologies are not enough. Companies and governments have to become far more informed about the issues, and deal with them in a thorough but pragmatic way.

Electronic Commerce – Greater Openness for Businesses

Ecommerce and the Internet has changed the way a company relates to it customers and to the public.

Customers no longer have to visit a branch or talk to company staff in order to do business with the company. Figures 1 and 2 show how things have changed.

In figure 1, customers have to do all their dealings through customer staff. That normally means they have to do it when the staff are available, and they probably have to go to the office where the staff and resources are located.

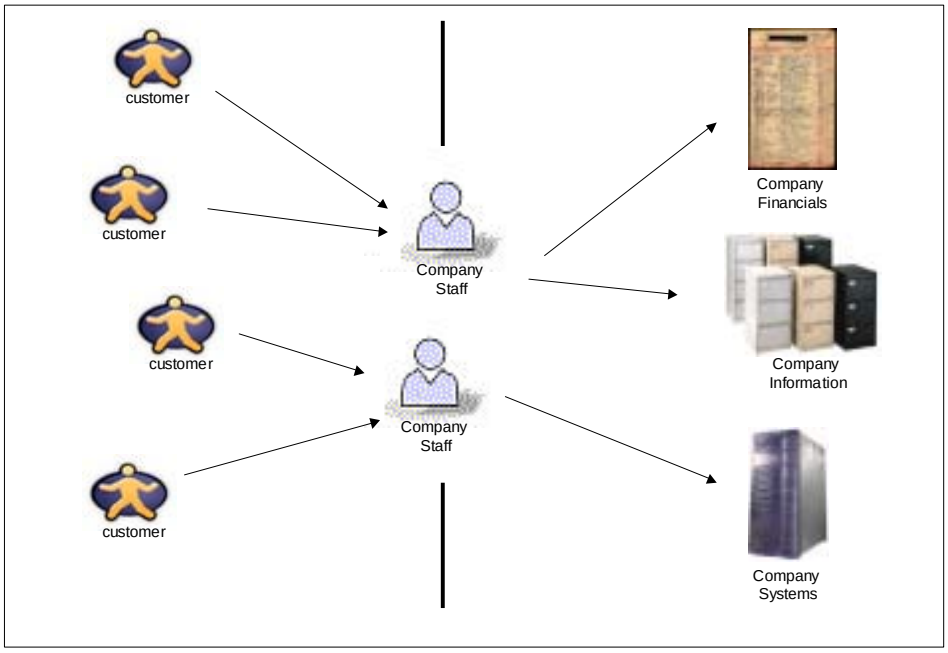

Figure 1: The old way. Notice how staff control access by customers and the public to the information and systems

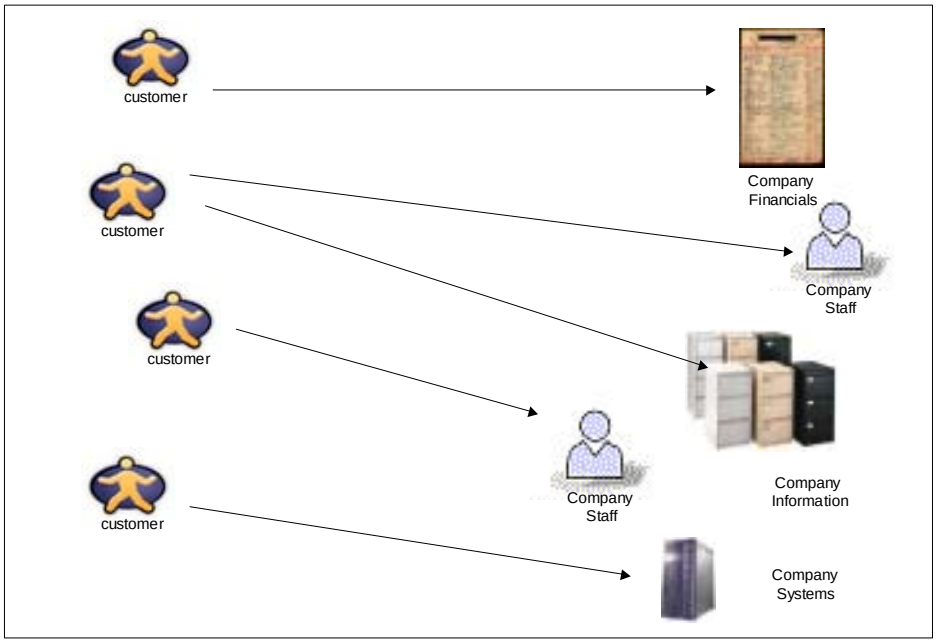

Figure 2: The New Way. Notice how customers access information and systems directly.

In figure 2, the customers have direct access, through the Internet to the resources they need. They can consult with staff if they need to, but it isn't strictly necessary. The old barriers between the customer and the company have begun to break down.

The change brings major benefits for companies and customers.

- It gives the potential for developing new business in new markets and operating in a very different, much more open way than previously. Barriers of distance and time-zone are overcome.

- It makes it easier to deal internationally. Long delays, postal and telephone charges and timezone differences are no longer such major issues. Being on the World Wide Web provides a shopfront for new customers to find out about the company's products.

- It improves customer service. Customers can take action for themselves, rather than having to wait on an operative. Customers can get up-to-date minute-by-minute information about things like pricing and inventory levels.

- Because it allows many functions to be centralised, it allows for much finer control of aspects of the business such as inventory and shipping. This frees up capital and allows the company to be more reactive to change.

- And of course, it reduces costs. It is now possible to keep your business open 24 hours a day, without having staff available at all times.

- For customers, it means that they now have direct access to their accounts and their information, without having to go to a specific premises at a specific time and wait for staff to be available. They can do their own business, from home or wherever they have happen to be in the world, whenever they want.

The same technology has also broken down barriers within companies. It means that colleagues from different offices and different countries can keep in touch and keep tabs on what is going on in each others projects.

It should go without saying that this results in profound changes in business. Barriers to entry, such as branch networks have become less significant. Customers have become more fickle and less averse to changing to a new, more competitive supplier. They may bypass local suppliers of goods and order them directly themselves from another country.

Vulnerability to Attack and Disruption

The same technology that allows you to remain open for business on the Internet 24 hours a day and breaks down the barriers between you and your customers (Fig. 2) also makes you much more vulnerable to electronic attacks.

As well as giving customers greater access, this new technology also potentially leaves them open to new forms of exploitation. Malicious people, impersonating users can get direct access to company resources and cause immeasurable damage. Equally, the company can be impersonated resulting in customers mistakenly disclosing confidential information to hackers.

The main focus here is on deliberate attacks on business. However, not all disruption is caused by attacks. Local flooding, lightning strikes, earthquakes, building accidents or accidental power outages can also cause serious disruption to a global business which is operated over the Internet.

Patterns of attack and disruption

So far, most of the attacks we have seen on information systems have been sufficiently small-scale that they do not make a major impact in the media. Many stories, particularly those involving fraud and blackmail are deliberately suppressed to avoid embarrassment. Very often, these stories involve insiders or disgruntled employees.

Many hacking occurrences do not cause very much damage. The perpetrators are often young people, who are exploring and experimenting. Even when they damage, they often do it because of foolishness or to show off their skill, rather than out of direct malice for the company effected.

Other attacks, such as viruses are very generalised, and do not often cause severe damage to any one institution or company.

One pattern we have not yet seen is concerted, politically-motivated terrorism with the intent of seriously destabilising an institution or country. In the present environment, it is quite likely that this type of attack will be attempted within the next few years. It will probably use a combination of different types of attacks to bring about its aim. For example, it might use a combination of targeted viruses and destruction of physical infrastructure to undermine a major institution, possibly with the help of 'sleepers' who have been planted inside the organisation. Clearly, this type of attack will need to be dealt with in a different way from traditional virus and hacker attacks.

National Implications

One of the places where the Internet has had the most impact, and where security is likely to be one of the biggest issues, is in the financial sector. The reasons for this are clear – money and other financial instruments lend themselves to electronic dealing, since there is no physical product to be transported.

The modern monetary system is dependent on digital information rather than on paper. If anything compromises or disrupts financial systems in a country, it also disrupts the flow of money in the economy. Clearly, this would have serious consequences for the whole economy.

Clearly, banking and financial activities are tightly intertwined with the economy of a nation or a region. Any serious damage to the banking system of a country will have implications for the perceived stability of that country and its currency.

This could have implications for a whole country, not just for a company. A major hacking attack on an egovernment website, or on a major commercial bank could easily lead to major disruption to public administration or even cause a loss of confidence in the monetary system.

Types of Attack

Most attacks are based on a few key strategies.

1. impersonating someone else, and submitting request on their behalf. The request might be to download valuable information, to buy shares, or to withdraw or transfer funds, or to order goods. It could also be to upload HTML pages to 'vandalise' a corporate website.

2. eavesdropping to pick up confidential information. They may use this information for other hacking attacks, or they may use it directly to get some material gain.

3. ‘denial of service’ where a system or network is temporarily damaged, resulting in disruption for customers

There are a number of ways these attacks can be perpetrated. Some of these are technical. For example, you may hear about a vulnerability in software which allows a particular type of server to be attacked. (For example, the CodeRed worm attacked certain versions of Microsoft IIS Server.)

However, many are social. According to Kevin Mitnick’s book, ‘The Art of Deception’, it is surprisingly easy for an outsider to ingratiate himself to a company’s employees sufficiently to convince them to install a rogue program on their PC, or to give out sensitive security information such as passwords or access numbers.

The language of computer security is full of jargon for describing different types of vulnerabilities.

Viruses

For example, you may be aware of the threat that famous ‘viruses’ such as Melissa and Bugbear pose. Most likely, some readers’ organisations have suffered serious disruption from these viruses. Hopefully, disruption was all you suffered. Viruses are computer programs that perpetuate themselves by taking advantage of features of Microsoft Outlook and Microsoft Internet Explorer. The virus is able to easily gain access to your browser and your mail client and use them to send infected emails to all the people in your address book.

In general, the viruses we have seen so far have been relatively harmless, compared to what could be possible. However, the real danger comes from the possibility of much more finely tuned viruses, which might be specifically targeted at your organisation. A virus like this would not be detected by regular virus-checkers, since it would not be internationally known. It might not cause disruption, but instead store and forward confidential information from your computer, especially passwords and key information. Viruses like this could ‘live’ on your computers for months without you discovering. The consequences could be tremendous, if the information can be used to access your systems from outside, or to allow junior employees to perform functions (such as purchasing) which they should not have access to.

Denial of Service

‘Denial of Service’ is a fancy technical term for an attack that causes your systems to become temporarily inoperable.

Typical examples of denial of service attacks are as follows:

- ‘ping of death’. There are a bug in certain operating systems which means that if the machine is not properly shielded by a firewall, it can be caused to crash from anywhere on the Internet using a special program.

- the ‘smurf’ attack. The smurf attack is a very clever attack that fools another network into overwhelming the target computer with traffic, causing it to become unavailable. The biggest problem with the smurf attack is that it is very hard to figure out who originally perpetrated the attack against you.

- Another simple “denial of service” attack is to simply overwhelm a web server with requests. This attack is quite difficult to perpetrate because you need to capture control of a large number of Internet hosts with access to a large amount of bandwidth. However, with some organisation, a terrorist organisation could probably do this (perhaps by spreading viruses, or perhaps by putting operators in place as low-level systems administrators in many different places around the globe.)

These types of attacks were used recently to attack the root name servers of the Internet. The ‘name servers’ are responsible for keeping track of where resources (such as websites or email servers) are located. If they had been further disrupted, the Internet would become practically unusable.

Routing attacks

Another major category of attacks is a routing attack. Routing tables are the underlying ‘glue’ which makes the Internet (or any network) operate. They are the ‘street signs’ of the Internet. They tell the routers what direction they should send the data in to go to a given destination.

It is quite possible to inject false information into the routing system, which will cause packets to be lost. It is very hard to track down the perpetrator of this type of attack, and it is very hard to fix while the perpetrator is still at large.

Power Supply

Another possible attack is to damage the power supply. In some cities, it is possible to cause major disruption to supplies by damaging the power network at only one or two points. A very determined hacker could even stop the operation of a backup generators if he could interfere with the supply of diesel.

Network Disruption

Another approach is to disrupt the network connecting the target organisation or computers to the Internet. This could be done through hacking into routing tables as discussed earlier, but it could also be done by breaking into other telephone company systems, or even by gaining physical access to the fiber optic cables.

Ripple Effects

Ripple effects are the indirect consequences of a hacking attack. For example, an ISP in Europe was hacked recently. The attack did not itself do much damage. But because the password database had been compromised, all customers had to be contacted to reset passwords. This upset customers, put enormous pressure on the telephone system and on the customer operations department It also attracted considerable media attention.

Much more complex ripple effects are possible. If a bank is disrupted, for instance, that may have implications for the cashflow of its customers, which may include other major businesses and ultimately their employees.

Dealing with the Threat

Although the stakes are incredibly high and we must be very vigilant, going back to a very rigid security policy is unrealistic. We cannot allow our business operations to be driven by paranoia. Companies have to be reasonably open to facilitate the services that customers now demand. They also have to be flexible. They cannot allow security considerations to overwhelm the development of new products and services.

The most common approach is to invest in technological solutions. The most common technological solutions are described below

Technological Countermeasures – using technology to fight the threat.

There are a number of technological approaches your company can take to help reduce the likelihood of hacking.

Diversity

Diversity means never being completely dependent on just one network connection or piece of equipment. This reduces the chances of a disaster if one of your means is infiltrated.

However, it is important that your routes are genuinely diverse. If your ‘diverse’ routes are all going through the same cable ducts, or cable ducts adjacent to one another, then you are still just as vulnerable to a deliberate attack. (A better idea might be to have a satellite circuit as an alternative.)

It could also mean having two servers with the same database on them. These two machines would then have to be kept synchronised. This is possible, but it is intricate, complex and expensive.

Obviously, if one machine is attacked and compromised by a particular technique, such as a virus or a DoS, there is a high likelihood that the other one will face the same problem. The design has to be very clever to avoid this possibility.

Diverse systems need to be tested regularly to ensure that the backup systems are working correctly and come into operation if there is a problem with the primary system.

Firewalls

Firewalls are a critical part of the security infrastructure. They basically monitor and filter data leaving and entering your company to ensure that nothing dangerous is allowed enter or leave your business's network. In practice, different firewalls operate at different levels. Some look at things like the type of traffic and the originating network. Others look 'inside' the message to try to determine whether to allow it through or not.

You shouldn't have firewalls only at the perimeters of your company network. Just as a ship is divided up with bulkheads to minimise the damage caused by any damage, so your network should be divided up into different sections. Quite likely you will need different rules around different parts of the business. For example, financial, legal and staff records need to be stored in a more secure part of the network than information about deliveries.

Firewalls need to be regularly updated and the logs they they generate have to be monitored.

Specific Measures, such as virus checkers

Virus checkers interoperate with firewalls and servers to check files for harmful viruses. They constantly scan all files, and if they find anything harmful, they remove the virus or put it in a safe place for detailed examination later.

However, virus checkers are very specific. They only check for viruses which they have been programmed to detect. They do not stop new viruses (until they have been updated) and they do not offer protection against other types of attack.

Cards with Magnetic Strips

Many systems (especially ATM systems and credit card systems) still depend on plastic cards with magnetic strips. PINs or signatures are sometimes used to strengthen the protection.

These types of systems are desperately unsafe. It is extremely easy to copy the magnetic strip on a credit card, and to use it fraudulently.

Surprisingly, credit card companies tolerate a certain level of fraud as a result of this weakness. This appears to be because of the time, cost and political difficulty involved in implementing a better system.

Public Key Infrastructure and Smartcards

Public Key infrastructure is a far more secure way of than passwords to secure transactions between you and multiple third parties. It works on the basis of mathematical principles, and providing certain rules are followed, it gives a mathematical guarantee that the message comes from who it says it comes from, and that the message has not been interfered with or read whilst travelling over the network.

Smartcards are usually used with public-key encryption to provide much higher levels of protection than magnetic-strip cards.

There are two main problems with Public Key Infrastructure.

- It may not be as secure as is sometimes claimed. There may be problems with the way the public key encryption is implemented. For example, certain types of smart cards can be copied and used for fraud, because of a fundamental design flaw.

- New techniques are beginning to emerge which allow this type of cryptography to be circumvented.

- The keys may be stolen without your knowledge. This makes the security useless.

- It is difficult and expensive to securely deploy in practice. This is because of the integration and training issues involved.

However, public key systems are by far the best hope for building a highly secure system with minimum vulnerability to fraud in the medium term.

Passwords and PIN’s

Passwords are the most common and best understood way to protect your systems. The concept of a password is very easy to understand for even the most lowly clerk.

However, passwords and PIN protection is often compromised. The most common reason is that the password is very obvious, or has not been changed from the default. Problems like this with PINs on voicemail and PABX systems in particular are quite common in Europe.

Most problems with website hacking (where websites become defaced) happen because of problems with protecting passwords. Quite often the password was very obvious. On

other occasions, the password was known to a disgruntled employee or contractor. Very occasionally, the password was ‘packet-sniffed’ off the network.

This is adequate for certain types of task, but it is definitely not adequate for financial transactions. In Singapore earlier this year, a keyboard-sniffing program (which stores all the keystrokes typed on a particular computer) was used in an Internet café to steal the passwords of bank customers. These details were then used to perpetrate a major fraud. Many banks avoid this type of problem by using ‘one-time password’ systems, or by only asking for part of the password for any one login session.

For most tasks, password protection is the best practical protection against impersonation. However, it is critical that:

- passwords are difficult to guess
- passwords are changed regularly

Biometrics

Biometrics means measuring aspects of the human body, such as the fingerprint or iris patterns to check that the holder of a token (such as an access card) is the same person who is using it.

Biometrics is a good idea, but it has key problems:

- It needs some form of key infrastructure to be in place before it can be implemented. (This is so that the biometric information on the card can be verified as being genuine.)

- It is not necessarily as reliable as people say it is. A Japanese study revealed that many fingerprint-based systems could be fooled with a false fingerprint made out of ordinary cooking jelly.

Another category of system sometimes called ‘biometric’ is face-recognition technology. This is now being trialled at airports in the US as a means to track terrorists. Questions have been raised in the media about how effective these systems actually are. These systems are certainly not yet accurate enough to authenticate users.

Locks and Concrete Walls

There are plenty of ways of penetrating a company other than getting in through an Internet. You could break into the office of the machine room through an access point.

Your network should be able to endure a reasonable level of physical attack. Locks and concrete, representing physical security are an important part of any network. If you want

the network to be secure, you have to keep doors, manholes, cabinets and any other ingress points locked.

What else can companies do to protect against attacks?

There is no 'magic bullet' to stop Internet attacks and hacking. You have to have a variety of approaches.

Every company and country that is connected to the Internet needs to consider the following areas:

- **education** – make sure your customers and your staff understand why security is so important and how the company's security systems work.

- **procedures** – make sure your procedures don't make it too easy for a customer or even an employee to do something that could be damaging. For example, your computer system might allow an employee to set an obvious password. Your system should not allow easily-guessed passwords to be used. Procedures for backups and business continuity need to be considered.

- **learn from mistakes**. Many hackers are opportunists, and are more interested in exploring your system than causing your company damage. If they compromise your company, it might be an opportunity to learn their techniques, before someone with more malicious intent finds your security weaknesses and does some real damage.

- **scenario planning**. Figure out some of the most likely scenarios for how your systems could be disrupted, and how your company would deal with them.

- **be a sensible consumer of technology.** Whilst security technology can be helpful, too much technology may give a false sense of security. It may also make systems more complex than they really need to be, introducing further dangers. Be careful about installing new software and consider the security problems that might arise.

- **not depending on the law and the government**. Policing your own network is your own business. You cannot expect the government to be able to protect you.

What can be done at government level?

Computer security is more than just a private or corporate problem. The consequences of a major hacking incident could be very severe, potentially leading to disruption of the money system and public services.

Governments and policymakers need to approach the problem differently. They must:

- **get the message out**. They must ensure that companies, individuals and state organisations know about the dangers and the importance of following security procedures.

- **monitor standards at critical institutions**. ensure that major institutions such as banks, power stations and hospitals have proper protection in place.

- **ensure that major institutions are not all sharing the same infrastructure.** For example, it may not be wise to allow a number of major banks to share the same data centre facility. Similarly, it might be unwise to have the entire public service connected into a single email system. (Of course the best solution for particular circumstances will depend on factors such as scale and type of installation.)

- **provide sufficient protection for critical national infrastructure such as fiber optic cables and power supplies**. This is critically important as the telecomms and power industries become increasingly deregulated. Undersea cables could be particularly vulnerable.

- **expect the unexpected.** Just as with the terrorist attacks on New York and Washington, future Internet terrorism will catch us off-guard.The government has to perform wider scenario planning to deal with attacks which could threaten national or international security. In particular, it has to consider the possible 'ripple effects' of an initial attack on a major institution.

- **Deal with the issues of law enforcement.** It is important that major problems can be tracked to their sources and can be dealt with quickly. For example, if a computer in your jurisdiction is used to attack a company in another country, it is important that your police force helps in dealing with the problem. Police forces need the resources and legal powers to get the information they need to stop a major attack while it is in progress. (However, this does not mean that you should tie up police time trying to track the perpetrators of minor hacking attacks.)

It is worth noting that the United States, through its department of Homeland Security and other initiatives is working intensively in this area. As the US becomes better protected, we can expect other countries to become more frequent targets. Countries outside the US need to act quickly.

Conclusion

The IT revolution has brought clear security challenges. We are vulnerable to types of attacks that we may not have considered before. We are still at an early stage of this revolution, and we do not yet really know what the extent of the dangers are.

However, we do know that there are dangers, and we know that there are people who would relish the opportunity to do serious damage.

We have to take a broad, wide-ranging approach to dealing with these problems. We have to implement technological solutions prudently and we have to train our staff and customers in using the technology and to understand the dangers.

Both companies and governments have to play their roles. On the one hand, corporations have to play their part by making sure their systems are secure and by continuously improving procedures. On the other hand, government has to facilitate the overall development of healthy a healthy security environment.

About Digital Messenger

Digital Messenger helps companies develop effective strategies for using technology to simplify and transform your business. Antoin O Lachtnain, the Chief Executive, has worked on Internet and technology developments with companies in Europe, Asia and the United States. In 2000, he was nominated as a ‘Global Leader for Tomorrow’ by the World Economic Forum.