COMITÉ EUROPÉEN DES ASSURANCES

SECRETARIAT GENERAL
3bis, rue de la Chaussée d'Antin   F 75009 Paris
Tél. : +33 1 44 83 11 83 Fax : +33 1 47 70 03 75
Web : cea.assur.org

DELEGATION A BRUXELLES
Square de Meeûs, 29   B 1000 Bruxelles
Tél. : +32 2 547 58 11 Fax : +32 2 547 58 19
Web : cea.assur.org

March 2003

Insurance and reinsurance of data losses caused by computer viruses

By Mr Peter Tailby Royal & Sun Alliance

Introduction

One of the basic precepts of insurance is spread of risk, the contribution of many to pay for the losses of a few. The global reach and the speed with which we can transmit information over the internet allow a virus to infect a vast number of computer systems and the networks they operate within. There is now a theoretical possibility that the propagation of a single virus or denial of service attack could result in claims on millions of insurance policies all over the world. The realisation of this theoretical possibility following the spread of the email virus " I love you" in 2000 has forced both direct insurance and reinsurance markets to analyse their exposure and clarify their intent under policy and treaty wordings going forward. This paper looks at some of the characteristics of virus propagation, the impact on commercial business and the potential for insurance risk transfer mechanisms.

Virus

The IT industry have never come up with a definition of electronic virus. We all know what a virus is even though we may not fully understand the underlying mechanism at work. There has been sufficient Media coverage over the last few years to raise the Public's awareness of the potential damage that viruses can cause. This awareness though has yet to prompt the widespread adoption of IT security practices.

Electronic Viruses are referred to by the way they spread or how they are launched. The collective term "virus" includes worms, trojans and logic bombs. Some viruses require the action of the recipient to begin infection and spread further, others can spread automatically from one system to another by seizing e-mail addresses for onward transmission.

In addition to virus we also need to consider two other activities that cause damage to data or compromise data flow through networks. The action of hackers targeting individual sites, defacing web sites, corrupting data or stealing information and Distributed Denial of Service attacks Ddos , that effectively block network traffic by flooding target servers with hundreds of information requests.

Not all viruses cause damage some are only a nuisance, but the number of attacks is increasing every year and the indications are that this increase is out pacing the growth of new websites and the expansion of the internet. However several automated tools are now available to would be hackers to probe websites and uncover vulnerabilities and this may go some way to explain the increase in the number of recorded attacks.

In addition to increased frequency, attacks through the internet are increasing in complexity and the latest attacks are designed to do the maximum harm. Called blended threats these new viruses spread automatically, they do not rely on user action to propagate, they have multiple attack methods and they can alter the way they propagate. Past infamous examples are “CodeRed” and “Nimda”. The latest, called “Bugbear” in addition to flooding e Mail systems and deleting files allows the hacker to monitor and control the activity of the infected computer system. Their ability to identify and exploit vulnerabilities and alter the way they spread makes cleanup much more difficult than single attack viruses.

Even encryption practices used to protect the most sensitive or critical data is being compromised by a new threat from Hackers called “side channel “attacks. Rather than trying to uncover the encryption key, hackers analyse how power consumption and processing time vary to identify patterns giving them clues to crack codes.

Sources of attack

According to the FBI/CSI 2001 computer security survey the majority of security breaches are caused by external attacks (70%) rather than internal from employees (30%). Conversely the financial costs of these internal attacks are much greater, almost 95% of the total. Employees have the specific knowledge of how to cause the most damage in addition to having easy access to computer systems. Of these costs losses from information theft and financial fraud account for more than 75%. Credit card theft represents 50% of the total. It is difficult to quantify the financial costs of viruses but these costs were significantly lower at 5% of the total.

We must consider all hacking attacks and viruses as malicious, but we should differentiate between activities of those groups who mean to cause real harm and those who are opportunist hackers (script kiddies) with limited experience who are acting irresponsibly.

Post September the 11th the former now includes terrorist groups and hostile nations, where the resources both in respect of knowledge and funding are available for a well structured attack which could seriously compromise security, defence, financial commerce and utilities of a target nation.

Cyber terrorism must be consider a possibility rather than a probability. The ability to launch an attack from a remote location is not so important if the perpetrators are prepared to sacrifice their lives if necessary to carry out an attack. The obvious intent of terrorism is to create terror and this works best when the targets are those that are the most symbolic of a nation's daily life. Although cyber terrorism could cause significant disruption it is currently unlikely to create sufficient trauma to achieve the terrorists objectives. This exposure will escalate in the future and in the USA in particular there is concern about the level of panic that could be created by a significant attack.

Future Development

Despite the downturn in world economies and the demise of the dot com entrepreneurs in the recent past, the use of information technology continues unabated as enterprise in general strives for a better understanding of business processes, to work smarter and improve efficiencies. Reliance on data and the networks transferring this information requires a thorough understanding of the vulnerabilities and security issues involved. The management skills and procedures to mitigate the consequences of information leakage and network failure will take on a greater priority in the future.

Although investment in these strategies is increasing, security practices still lag behind the implementation and expansion of information systems. Companies are reluctant to sacrifice network efficiencies caused by incorporating security procedures. Security slows down the internet and efficiency reductions of up to 25% can be experienced in some circumstances. Vulnerability assessment and risk management procedures, both at the user, software developer and service provider levels need to be stepped up to reduce the likelihood of an event occurring and to mitigate the damage when it does occur.

Transaction and process verification initiatives such as Digital Rights Management (DRM) and Microsoft's Palladium will go along way to prevent identity theft and unauthorised access to personal data while on the internet and other networks at the operating system and application software level. Awareness at the user level is also improving to some extent. Although employees realise the need to use passwords, to keep them confidential and avoid opening unidentified email attachments, these procedures conflict with daily work and are some times ignored.

Insurance Policy Wordings

Potential losses from virus damage were not contemplated when material damage policy wordings were formulated, partly because the exposure had not been recognised and partly because the loss experience in the past had not been significant. In most European countries corruption of data had not been considered a covered cause of loss because the operative clause referred to physical loss or damage to tangible property. Data was not considered to be tangible property and data corruption was not considered to be physical damage. In the UK this was a less secure defence as the standard all risk property policy has an " all other contents clause " which is left undefined and could be construed to include such intangibles as data.

Legal rulings particularly in the USA market indicate that reliance on the limitations of the operative clause will no longer be an adequate defence in the future.

Alerted to this potential exposure Insurance market representative bodies advised their membership that modifications would be required to standard wordings to ensure that cover for these types of losses was not given unintentionally. In Germany clause 28 which was a common endorsement to Electronic Equipment policy wordings provided costs for manual re- entry of lost or distorted data from a range of causes including virus. The German Insurance association GDV advised their membership of the potential accumulation problem and subsequently modified the clause 28 to read " Regardless of other contributing reasons the insurer does not indemnify for distortion or loss of insured data or programmes that have been caused by programmes or data with loss causing functions such as computer viruses, worms, trojan horses (unless otherwise agreed). It has to be added that malicious acts committed by third parties namely intentional modifications in programmes and data are not excluded in general, unless the loss is caused by viruses, worms or trojan horses. The German market has taken a cautious approach and in practice only limited cover is provided with low loss limits for virus and hacking attacks. Denial of service attacks are not covered.

In the UK the Association of British Insurers equally advised their membership of the potential accumulation problem and devised alternative modified wordings in conjunction with legal advice from Cameron Mckenna to exclude damage to data caused by virus and hacking. Two alternatives were put forward, one to exclude damage to data and the other to exclude damage to data caused by virus or similar mechanisms. See appendix 1 Definitions

UK Engineering Computer policies specifically provided cover for data damage with an additional cover for virus seek and destroy costs. Excluding all damage to data would seriously affect the viability of such a policy and the option to exclude damage caused by Virus or similar mechanism only was suggested for this type of policy.

The approach in the UK market to date has not been consistent. Some carriers have applied exclusions since the first quarter of 2002. Others have chosen to remain silent on the issue and others provide cover subject to a loss limit and specific risk management requirements.

Reinsurance wordings

The reinsurance market was the first to take action on eRisk exposures by alerting their cedants back in 1999 that treaty wordings would exclude virus covers from the 2000 year renewal season. This position was not prompted by loss experience but by the shear size of the potential worldwide aggregated exposure from such an event.

Munich Re issued a clarification wording that was to be applied to Property, Liability and Engineering treaties from 2000 year onwards. Other market reinsurers including Lloyds also introduced exclusion wordings. Lloyds NMA 2914 and NMA 2915 were adopted by most UK markets on subscription business in early 2001 as an interim measure whilst they developed their own clauses.

Exclusion wordings now appear on nearly all reinsurance treaties and this situation is not expected to change significantly during 2003.

Risk Management Requirements

Risk management requirements and procedures need to be tailored to the specific conditions of individual risks and their reliance on data and network integrity, there are however some basic criteria and practices that apply to all commercial operations to reduce potential damage from viruses as follows:

Entry points to IT systems and networks need to be secured to prevent authorised access. This ranges from physical restrictions to computer terminals to configuration of firewalls, anti virus software and encryption techniques.

A well configured network linked to the internet would include multiple servers load balancers, with multiple firewalls and antivirus protection, caching of non critical data, encryption of critical information and intrusion detection systems to monitor network traffic flow and prevent onward transmission of potentially malicious code.

These levels of protection do require dedicated IT staff which would be outside the resources of most small to medium enterprises. In addition the more security procedures there are in a system the greater the reduction in the efficiency of the data flow creating additional costs to maintain functionality over and above the direct costs of security.

For small to medium enterprises there are basic security strategies that can be incorporated at reasonable cost that would go along way to minimise the impact of a virus attack.

The first of these is restricting physical access to computer systems by securing the buildings or rooms housing the equipment to prevent potential attackers getting access to terminal keyboards. The use of eight digit alphanumeric passwords that are changed on a regular basis will also deter would be attackers.

Electronic security is also required with a combination of firewalls and anti virus software. The firewalls controlling data traffic flow to and from the server should be correctly configured. The default passwords supplied by the manufacturer should be changed and unwanted services disabled to make it more difficult for back door attacks. Anti virus software should be installed and updated on a regular basis, preferably automatically from online downloads.

Operating and Application software security patches are regular released by the software manufacturers shortly after a vulnerability has been identified. These security patches should be downloaded promptly to prevent hackers exploiting a newly identified vulnerability.

Data back up procedures also take on a greater importance. Transaction data should be backed up daily and stored offsite and a current copy of the operating and application software should be stored at a remote location.

Management procedures should also be in place to raise employee awareness, stressing the need to keep passwords updated and confidential, and to not open e-mail attachments with the common file extensions .exe, .bat, .vbs, .pif and . scr. Employees should also be instructed in what actions should be taken when a virus is identified to reduce the likelihood of onward transmission throughout the network.

Conclusions

Markets do exist for the provision of eRisk covers including virus exposure, particularly from the Lloyds market and American Carriers but these policies concentrate on larger risks and are subject to extensive risk management surveys by specialist IT companies. These are expensive to administer and to a great extent can only reflect the protection levels in place at the time of survey. With such rapid developments in technology, the rate of change of the exposure profile is probably too fast to keep underwriting evaluations up to date. In addition these types of accounts are biased towards the high risk exposures where there is an evident exposure and consequently a certain degree of selection against the Insurer.

There are also difficulties in establishing the insurable value of data, historically this has been written on a first loss basis, which bears little relation to the exposed value. A better valuation can be obtained by establishing the installed storage capacity in megabytes and agreeing the proportion of "data worth restoring" with the insured. Typically this proportion amounts to less than a few percent. With the high storage capacities currently available, particularly in the desktop environment, this assessment method also has its flaws.

In addition, establishing the cause of loss in the event of a claim can be difficult and IT specialists will be needed to carry out investigations in complex situations.

Small to medium enterprises on the other hand probably represent a more viable sector for the provision of virus cover. Provided the basic risk management requirements referred to above are implemented before the inception of the policy and businesses that are wholly dependent on the internet are avoided, the impact of virus damage should be minimised to an acceptable level for underwriters. Acts of terrorism and DdoS attacks would still need to be excluded, as these events are much more difficult to defend against compared virus and hacking attacks.

Aggregations will need to be carefully monitored both in terms of the accumulation of multiple insureds relying on the same internet service provider in addition to the stacking of the policy loss limits per event.

At this point in time there has not been enough experience to accurately set PMLs for virus as there have been very few cases of actual insured losses in the past. The insurance industry will however need to develop these tools to respond to the Insured's needs as their network and data dependencies become more critical in the future.

Appendix 1 Definitions

Commission of the European Communities definitions

(a) ‘Electronic communications network’ means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting , and cable TV networks, irrespective of the type of information conveyed.

(b) ‘Computer’ means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data.

(c) ‘Computer data’ means any representation of facts, information or concepts which has been created or put into a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function.

Illegal interference with Information Systems

Member States shall ensure that the following intentional conduct, without right, is punishable as a criminal offence:

(a) The serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data;

(b) The deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system where it is committed with the intention to cause damage to a natural or legal person.

UK ABI definitions:

Material Damage:

The Company shall not be liable under this policy in respect of loss of or damage to Computer Equipment, Auxiliary Equipment or Computer Media directly or indirectly caused occasioned by or arising from Virus or Similar Mechanism or Hacking

Additional Expenditure:

The Company shall not be liable under this policy in respect of additional expenditure in consequence, directly or indirectly, of Virus or Similar Mechanism or Hacking

Virus or Similar Mechanism:

Virus or Similar Mechanism means program code, programming instruction or any set of instructions intentionally constructed with the ability to damage, interfere with or otherwise adversely affect computer programs, data files or operations, whether involving self-replication or not. The definition of Virus or Similar Mechanism includes, but is not limited to, trojan horses worms and logic bombs

Hacking:

Hacking means unauthorised access to any Computer Equipment, Auxiliary Equipment or Computer Media, whether the property of the Insured or not