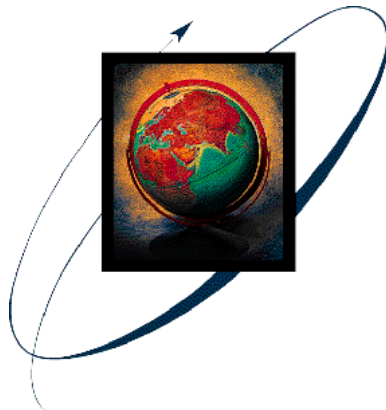


Creating the Market for Intermediating Digital Risk

The Changing Risk Landscape:
Implications for Insurance Risk
Management. 1999.



Job Maats

AON

ABSTRACT

Consolidation, globalisation, new technology, and decreasing profits are reforming the insurance industry. To succeed in this new environment, (re)insurers have to pursue innovative ways to increase the bottom line. Advances in information technology are radically changing the way many businesses operate, giving them the ability to provide better quality products at a lower cost. A new age of risk is emerging that coincides with the explosion of reliance on computer-based technology. Digital risk can be defined as the risk that a digital machine (that is, a computer system) does not produce the scheduled accurate result within design specifications. Some elements relating to digital risk are unfamiliar to the insurance industry and, hence, are creating a challenge for that industry to produce insurance products that match the risks.

INTRODUCTION

Globally, all commercial sectors have come to rely on computer-based technology in one form or another. It is apparent that technology is now capable of providing and undertaking processes that are more efficient and effective than if done manually through direct human input. In order to maintain competitive advantage, it is now imperative for businesses to use information technology to provide better quality, scope, and delivery of service. As a case in point, it has been:

... noted that the number of Internet users making purchases over the Web is expected to jump from 31 million in 1998 to more than 183 million in 2003. According to International Data Corp., the amount of commerce conducted over the Internet will exceed \$US1 trillion by 2003 (*EDS New Release*, 21 July 1999, p.2).

The down side to this revolution is that 'information age' businesses have no option but to open themselves up to digital risk in the day-to-day running of their business. There is a general rule for net-based businesses that for every hour of downtime, a business relinquishes approximately 1% of its share value. Companies clearly have a problem with business interruption, and thus want to have cover for this type of risk beyond the products the insurance market currently offers. The move away from manufacturing to service-based industries requires far more reliance on intangible, rather than tangible, assets. For example, while Microsoft's market value is estimated at \$US500 billion, only about \$US1.5 billion on its balance sheet relates to property and

equipment (*Microsoft Annual Report*, 1999). As long as the insurance industry continues to focus on traditional physically triggered risks, it will miss out on meeting the true insurance requirements of modern corporations, which commonly relate to intangibles such as intellectual property rights, reputation, and brand value.

The insurance industry has provided risk management benchmarks and best practices throughout the industrial age, based primarily on the needs of its clients. Now, however, insurance companies must look to new horizons with a view to expanding and providing new product suites that meet the needs of the information age customer. It is for this reason that the entrepreneurs involved in MorpheX (Bermuda) Ltd., the world's first digital risk service reinsurer, have devoted most of the 1990's to building the specific knowledge and identifying the innovations required to create a new market infrastructure for economic coordination between (re)insurers, brokers, and the software market.

This paper will provide an explanation of digital risk, some of the prerequisites, and some of the problems associated with writing digital risk cover. Finally, an example, based on the Microsoft NT operating system, will be used to illustrate how digital risk triggers will specifically work in the case of this system.

AN EXPLANATION OF DIGITAL RISK

Computers have been around for over 50 years, however, the risk associated with them is only now becoming an issue for the businesses who rely on this technology. Before an explanation of digital risk is given, an understanding of 'digital machines' is essential for comprehending the problems associated with this type of risk.

Digital Machines

Digital machines operate through data series or systems of digits. Each machine is made up of four elements with a specification and implementation program. The four elements (or inputs) include a hardware component, a software component, human input, and data. Each of these elements is subject to both specification and implementation errors. In other words, each of the four inputs can fall below operating expectations due to wrong design or incorrect implementation of the design. The degree to which any of them fall short (do not meet operating requirements) is intrinsically unknowable. It is possible that over time confidence intervals showing the frequency of errors (downtime for each component of a digital machine) could be estimated. However, the severity of failure at the tail (percentage of downtime for each component over an extended period of time) will never be learned.

Electronic errors can be defined as outcomes not permitted for a particular component and/or outside what is anticipated for a specific digital machine. The digital machine's exposure to errors is magnified by the fact that the four

elements that make it up operate serially rather than in a parallel fashion. As a consequence this means that any one error would affect the whole system, not just the component it originated from. Thus, the overall strength of the system is only as strong as its weakest link.

Errors can either trigger a crash of the digital machine or the machine can produce an outcome where confidence in its accuracy would be misplaced. Errors transmitted to a successive component, either within the same element class (for example, an error in the software component multiplying within the component) or in a different element class (for example, the same software component error procreating in a data series), can create wholly unpredictable behaviour. This is a consequence of the generic multi-purpose nature of most components that make up most digital machines. An example of a generic multi-purpose component could be Microsoft Office Suite software.

Digital Risk

Digital risk can be defined as the risk, or the probability, that a digital system (or single machine) does not produce the scheduled accurate result within the processing specification (capacity) of a machine. Well-designed digital machines are capable of producing consistently accurate results. Repetitive uses of all four underlying components (hardware, software, the user, and data) have, by and large, revealed most implementation errors over time. Thus, accuracy of individual components tends to be high. This is especially true of software and hardware components because the cost of fixing errors in these areas, once detected, is relatively low compared to a manufacturer's reputation for that component's reliability. However, Foote and Huebner at the University of Texas (Austin) comment:

Different computers may not have the same capability to perform complex mathematical operations and may produce significantly different results for the same problem. Burrough (1990) cites an example in number squaring that produced a 1200% difference. Computer processing errors occur in rounding off operations and are subject to the inherent limits of number manipulation by the processor (Foote and Huebner, 1995).

The elusive circuitry error in the Intel Pentium chip (see Markoff, 1994), that caused inaccurate results to be generated and that was widely reported, is a representative manifestation of the above problem.

The Year 2000 (Y2K) computer problem has highlighted the fact that computer systems can and will continue to have design and implementation problems regardless of how well planned they are. The Gartner Group, for example, calculates that litigation, with regard to Y2K in the USA, could surpass \$US1 trillion, not including the \$US600 billion plus figure to literally correct non-compliant Y2K hardware and software systems before the end of 1999 (McNee and Keller, 1997). Y2K has done a remarkable job of sensitising businesses to the risk associated with computer-based technology. In the

context of identifying new insurance business opportunities, Y2K has mostly been good news for the insurance industry, as the importance of cover has been established. However, insurers will not generally be required to respond to Y2K claims.

Other design and implementation problems like Y2K may lie in wait. Digital authentication systems reliant on light-weight, decades-old encryption routines running on operating systems that intrinsically lack security are at risk from massively failing their owners whenever the next breakthrough in computing power takes place. The consequences of mass intrusions into financial systems at that time could exceed the cost of Y2K.

Soft targets in an interconnected world should not expect insurers to pay for the consequences of having their systems hacked into when deploying encryption keys of inadequate length. Due to the types of cover being written in today's market and the speed by which these types of problems will creep up on many insureds, they may well believe themselves to be covered for such risks. Insurance policies insist on adequate physical protection of assets through deployment of sound locks, as such, similar protection for computer systems through the adequate length of digital keys may not be required.

Even the best digital systems still have an estimated 0.4% error rate after extensive testing of their software code. In other words, for every 1000 lines of instructional (source) code for a specific software application, four will contain a mistake that may create problems for the user by completely failing or not performing operations as expected. Given this environment, it is fair to say that all software at the time it is being used and even at purchase is intrinsically defective. The consequences of these defects for the business community are that one should anticipate some economically unscheduled downtime of digital machines and/or the allowance in production of inaccurate output outside the specified range.

There is no question that commerce has come to rely heavily on electronic services. This has reached a point where many organisations do not have sufficient manual back-ups to adequately sustain output if it becomes necessary. Hence, an unscheduled disruption automatically reduces service and product delivery and, therefore, profit. As such, there is a large, continually growing market for covering/insuring against digital risk that is becoming increasingly important to the welfare of businesses who are unable to financially survive prolonged digital machine interruptions.

DIGITAL RISK AS AN INSURANCE PRODUCT

Traditional classes of risk, such as severe weather and infrastructure failure, are also capable of influencing the accurate and timely operation of digital machines. However, unlike conventional insurance, no physical trigger, for example, a hurricane or earthquake, may be apparent for digital risk to occur. Although the interference to a computer system is less obvious, it may create

the same amount of interruption through downtime, systems failures, and inventory disruption.

As mentioned earlier, there is a prevailing rule for internet-based businesses that for each hour of business interruption there is about a 1% erosion in the share price for that company. It is against this background that businesses need to insure against digital risk and potential monetary loss. Interruption of service creates a natural basis to attach insurance.

Loss-adjustment on the basis of the number of elapsed minutes of downtime multiplied by a compensation rate per minute of such downtime appears to be the logical basis to indemnify actual losses suffered (see Figure 1). However, this needs a highly sophisticated global time stamping and messaging infrastructure to monitor insured machines worldwide. It also requires ensuring that financial capital providers are satisfied that processes are in place to secure an early recovery in order to contain and terminate loss. This requires a tripartite relationship between the digital risk insurer, the service provider, and the insured. This

Figure 1. Formula for Calculating Digital Insurance Payments

$$\text{Digital Insurance Claim Payment} = \text{Number of Minutes Downtime} \times \$ \text{ Compensation Rate per Minute}$$

would enable the digital risk insurer to financially warrant the time-to-fix performance of a service provider under a service level agreement (contract) in favour of an insured.

Relevant Regulations

Under European Union (EU) regulations insurance has become formally coded into 18 specific classes (some identified over 100 years ago), which conventional insurers believe define the entirety of the insurance business. These classes have all been explicitly linked to the regulatory framework. Anyone writing these classes of insurance requires a licence.

Without such a licence, EU directives are infringed. Digital risk was not anticipated and, thus, does not fall into any one of these categories.

As the EU operates under a civil law framework (which in essence means that if it is not forbidden, it is not unlawful), writing digital risk cover in the EU without an insurance licence is, therefore, not illegal. The latest round of financial intermediation deregulation by the World Trade Organisation (WTO) means the EU and other jurisdictions are unlikely to stand in the way of corporate businesses purchasing non-consumer digital risk from outside their 'home' territory. Given this, digital risk is capable of developing from inception as one global market with operations concentrated in one, or possibly a few, geographical centres.

Defining Triggers

The conventional insurance industry's basis for making payments for hundreds of years has been to respond to physical and legal triggers. A change in the environment within which businesses operate means that these traditional triggers are no longer wholly adequate for defining insurance related events. The new era of information technology means that there is a need to re-design the boundaries about how insurance payments are triggered. Digital risk is a good example as it is qualitatively different from conventionally triggered risks and requires a new approach to claims administration and adjustment. In essence, computer systems, the majority of the time, do not stop operating because of traditional physical and legal triggers. Rather, the triggers that cause disruption are undefined, vague, and unpredictable. The fact that you have to define the triggers creates a new set of legal problems because it is necessary to address from where insurance payments originate, since the triggers that produce computer system downtime can not usually be identified. Insurance carriers, therefore, need new forensic monitoring systems to be able to adjust digital losses.

Problems Associated with Insuring Digital Risk

As with any new, or even old (for example, flood), field of risk there are many problems associated with insuring and pricing the risk appropriately. With no historical data to help define digital risk and its impact on business, the task of suitably quantifying this risk is far greater.

As mentioned, the triggers that define an insurable event with digital risk are vague and poorly defined. Thus, there is an undeniable risk in relation to moral hazard and, in particular, fraudulent claiming. In the case of moral hazard, potential insurance carriers need to be mindful that users (one of the digital machine components) may not change their behaviour towards taking preventative action with regard to computer downtime. The problem then for insurance carriers is how to make sure that this type of behaviour is kept to a minimum. One answer could be the use of incentivisation. If users are incentivised to act in a certain way, in this case preventing downtime, there could conceivably be a change in performance.

The problem of fraudulent insurance claiming with regard to digital risk is more complicated. If a business is insured against downtime in its computer system, what measures are there to stop the insured unplugging a computer and making an insurance claim for business interruption? The solution to this is effective time stamping and messaging infrastructures.

The actuarial data deficiencies in digital risk are similar to those encountered in the financial markets with 'value' at risk. Prodigious amounts of data are available for short-term business interruptions. The economic damages from these short-term interruptions are, however, insignificant. This type of digital problem can be cured at low cost by clustering and providing modern operating systems with faster reboot times. There is very little statistical data with regard to longer business interruptions. Carefully monitored historical behaviour, in terms of reboots, can be indicative of stability or lack thereof and, thus, can inform through simulation based on historical analytical data. Combined with a fair degree of judgment these quite complex risks can then be underwritten.

Pricing of Digital Risk

It is not difficult, given the problems outlined above, to imagine that digital risk is not only almost impossible to quantify, but that the pricing of such risk has an inherent lottery element attached to it. As with any risk, digital risk must be priced by the insurance industry to provide sustainable long-term rewards in return for the willingness to underwrite this potentially catastrophic risk.

The economic efficiency and low friction costs created by electronic commerce businesses has large rewards for those who are able to decompose associated risks and disintermediate. For these businesses there is a necessity to avoid carrying digital risk and, thus, also the need to use scarce external financial capital to support such risk.

From a (re)insurer's point of view, the goal to effect pricing of digital risk is to have an open, but very structured system that will analyse each claim and determine its integrity. The system would also need to be designed in such a way that all parties (brokers, (re)insurers, capital providers, insureds, and component developers) are all focused on mitigating risk and, hence, mitigating the cost of eventual losses. The most likely solution would be to have co-written insurance policies between suppliers, manufacturers, and (re)insurers.

An Illustrative Example: Microsoft NT Operating System

The current version of the Microsoft NT operating system has some 14 million lines of instructional (source) code, which is expected to increase to 44 million in the next version released. This system, working in conjunction with a hardware component, currently offers 15 services to application software machines. However, if one of these 15 services is not available the digital machine will not function as it was designed to. Thus, the availability of the NT operating system is defined as being capable of meeting expectations only when all 15 services offered to applications running on the NT platform are actually working.

These 15 services can be monitored for their continuous presence to signify that the operating system is running on a specific hardware component in a specific location and is, hence, able to produce specific outcomes at designated times. It is possible (using a series of complicated mathematical formulae) to come up with an estimated figure of downtime of the NT operating system. However, it is impossible to forecast what effect the other three components of a digital machine will have on business interruption when they all interface and co-exist as one machine.

To provide insurance cover for such a system, a combination of monitoring and messaging of the insured machine would need to be put in place. Insurance would also require site examinations on the design and output capacities of the specified machine so that a comprehensive understanding of the risk of business interruption is appropriately priced and within determined boundaries.

CONCLUSION

Limited knowledge of digital risk within the conventional insurance industry and the lack of qualification to professionally underwrite such risk almost certainly prevents significant digital risk coverage becoming a viable product through traditional systems. The key will be creating new information age technologies to make these risks readily comprehensible, to (re)insurers and insureds alike, to create economically viable options for these potentially catastrophic financial risks.

REFERENCES

EDS News Release. 1999. EDS Playing Key Role in Defining E-Commerce Policies. www.eds.com/news/news_releases. July 21: 2.

Foote, K.E. and Huebner, D.J. 1995. Errors, Accuracy, and Precision. The Geographer's Craft Project. Department of Geography, University of Texas. Austin.

McNee, B. and Keller, E. 1997. Year 2000 Projects: A Race for Funding. Inside Gartner Group This Week. October 29.

Markoff, J. 1994. Circuit Flaw Causes Pentium Chips to Miscalculate, Intel Admits. Times News Service. November 24.

Microsoft Annual Report. 1999. Property and Equipment. www.microsoft.com. June 30.

The views expressed in this document are those of the author, and not necessarily of Aon Re Australia Limited. The papers are intended to provide general advice in summary form. The contents do not constitute advice and should not be relied upon as such. Formal advice should be sought in particular matters. Aon does not provide warranties, guarantees or undertakings in relation to the accuracy, completeness or currency of the information provided and does not invite reliance, or accept responsibility for the information being provided.