

## MANAGING RISKS IN THE GLOBAL INFORMATION INFRASTRUCTURE

### Corporate Information - Confidential Asset Or Leveraged Resource?

a paper presented to  
the Australian/OECD Conference

on

## SECURITY, PRIVACY AND INTELLECTUAL PROPERTY IN THE GLOBAL INFORMATION INFRASTRUCTURE

7-8 February 1996

Canberra, Australia

by

**Professor Shane Simpson**

Director

**Technology Risk Management Centre**

Faculty of Law

University of Wollongong

### Introduction

The economy of Australia, and many other countries, is hugely influenced by the mining and sale of primary resources: iron ore, coal and oil deposits are highly valued and extensively exploited. Their absence or presence are recognised as being essential to the evaluation of any economy. Despite our expertise as quarrier, we have overlooked one of the great deposits of primary material - corporate information.

One of the community's most important under-utilised resources is that wealth of information owned and protected by corporations and governments for their own use ("corporate information"). Every company and every government department holds deposits of corporate information. Some of this might be best thrown out but much of it could be more efficiently and productively exploited.

The recent technological developments in communication technologies have encouraged, indeed enabled, the globalisation of the information market. Perhaps until technology gave us an efficient means of access to and dissemination of information, there was little opportunity of developing a market for corporate information. The Internet and other on-line communication technologies have changed that.

### Corporate Information As An Asset

Generally, corporate information is one of the core assets of any corporation or government.

Traditionally, owners have protected the perceived value of their corporate information by resisting its disclosure.

Perhaps because of its relationship with the decisions that should have been made, were made or are yet to be

Liability limited by a scheme approved under Professional Standards Legislation. Simpsons Solicitors Pty Ltd (ACN 125 211 823) trading as Simpsons Solicitors.

made, we are uncomfortable with disclosing corporate information. We have a propensity to accumulate it, store it and protect it. Whether it is overwork (which is understandable), the fear of competition (which can sometimes be commercially justified) or the obstruction of review and criticism (which can rarely be in the public interest), owners of information have generally taken the view that corporate information must remain confidential to the corporation.

My suggestion is that the advances of communication and information technology now permit us to take a bolder view; a more creative view: yet one that is economically, corporately and socially responsible. In brief, there is the potential for considerable public and private benefit if information is seen as a commodity, which is available, which is accessible, and which is valued.

I am not advocating a throwing open of the vaults; a granting of unstructured access to all who ask. Rather, because of the value of the corporate asset, owners must develop risk management protocols to protect and enhance the value of their information. This will demand a rigorous examination of the latest technology to assist in the difficult process of structuring, ordering, sign-posting, storing, protecting, retrieving, revealing and, perhaps, being paid for, the asset that is corporate information. None of this is useful unless the integrity of the information is assured, possession and control is maintained and payment procedures are enforceable and secure.

Information access also demands an equally rigorous examination of the human administration procedures involved. Any organisation that is moving from an archaeological model of information handling to an access model, will necessarily need to adopt new management techniques for protecting its on-line intellectual property.

### **Towards A New Approach To Information**

Quite simply, information owners must analyse the value of their information assets more closely to determine more accurately whether confidentiality is worth maintaining at all, and if so, what degree of confidentiality should be conferred.

Part of this analysis must be an evaluation of the possibility of **leveraging** that value: exploiting the value of the information.

In this way, the corporation benefits by exploiting its hitherto unrealised information assets and the community at large benefits by having a hugely magnified information resource. We often hear that "there is no point reinventing the wheel" yet that is exactly what our present attitude to hoarding information obliges us to do. Our attitude should be not -

"I have invented the wheel; this gives me advantages so I will not share it" but rather -

"You may have access to my wheel but the extent and the terms of that access will be a matter for our mutual advantage".

### **Reasons For Granting Third Party Access**

There are many reasons why a company or a government department might want to do this.

## **Attracting new clients and enhancing client loyalty**

For companies (and for government departments that have been corporatised), granting a client the privilege of access is one way of attracting and retaining the loyalty of that client. Indeed, the level of importance of the client (or the targeted potential client) may be reflected in the level of access granted.

Such access can be marketed as:

- (a) a value-added to the traditional service offered to clients;
- (b) a service that is not offered by competitors;
- (c) an acknowledgment of the importance, the "special status", of the client.

As such, it can be presumed that such access makes the corporation's services attractive, promotes loyalty in existing clients and, eventually, client dependence. All of these would be recognised as commercially advantageous.

## **Creating A New Market**

At the moment, the traditional view of corporate information is that it is one of the intellectual resources that gives the organisation an advantage over its competitors. The new technologies are forcing us to critically evaluate this view.

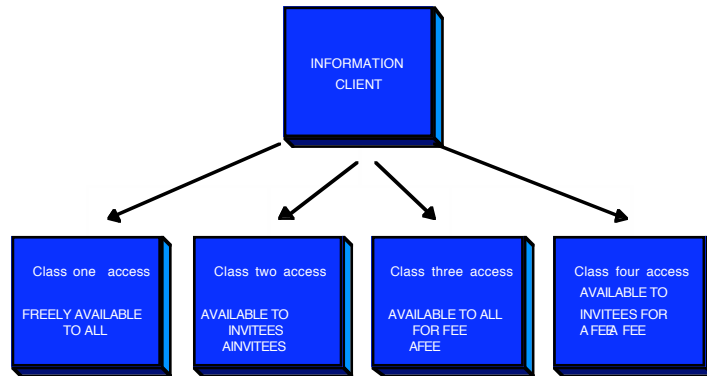
By way of example, let us consider the Attorney General's Department of the Commonwealth Government. It has recently been corporatised; its legal advice givers must now time record and time charge; government instrumentalities may now retain outside law firms for certain types of advice if that course is seen as more cost effective or efficient. Now, many of the legal advice functions of the Attorney General's Department are in direct competition with the private sector.

Within the Department, there is an enormous wealth of accumulated information. The Department now has a choice: does it hold its corporate information to its bosom on the basis that this corpus represents an advantage over its commercial competitors or does it adopt a new approach: one that would have been almost impossible to effectively administer, just 24 months ago?

Why not open up the vault of knowledge?

By way of illustration, a simplified model might look something like this:

## VARIABLE ACCESS STRATEGY



In such a model, access is not a blunt instrument. It can be granted according to various classes of invitee and on various terms.

For example, assume that government lawyers have written an opinion as to the meaning of a particular statutory phrase. Rather than adopting the traditional archaeological approach to such information, why not leverage it by turning it into a product? The Department might choose to keep the advice confidential until its immediate purpose is complete but then, it may make it available on the “fee for access” database. If it existed, one of the resources that any law firm would have to utilise would be the “AGLAW On-line Services”: What litigants could resist buying a relevant opinion from such a source? The Department may sell that advice many times over.

What are the advantages to the owner of the information?

**CORPORATE ADVANTAGE**

- ▶ one exercise of intellectual effort
- ▶ limited promotional costs
- ▶ 24 hour client access
- ▶ international market
- ▶ minimal distribution costs
- ▶ fully computerised financial administration, and
- ▶ no limitation on the number of times that same material may be sold.

It is a classic example of the advantage of selling bits rather than atoms. This is true leverage.

### Public benefit

It has been said that “knowledge is power”. In fact, the mere possession of information is rarely empowering. All too often it is merely a storage problem.

The **public** benefit is perhaps best gained by increasing access to the various repositories of accumulated knowledge. More important than who owns and controls the information, is its relevance, its newness, its cost, its accessibility, its potential for application and the opportunity for its further development.

I am not arguing that copyright is no longer relevant or useful. The argument in support of structured access to corporate information applies whether the information is protected by copyright or not. Nor am I entering the debate as to the desirability or otherwise of government using statutory licences or exceptions to promote the public interest of accessibility and thereby diluting the degree of control that would otherwise be conferred by copyright ownership. Rather, I would suggest that if we rethink our attitude to the value of corporate information, we will find that an individual corporation's commercial interest and the public interest are often compatible.

## **Reasons For Not Granting Third Party Access**

There are many circumstances which will demand that the owner will chose not to grant third party access to corporate information. The following is just a sketch of three of these situations: 1. *Information that commercial interests demand be kept secret*

An example of this is where the corporate value of the information has not yet been exploited by its owner: Take a company that has blueprinted the genetic structure of a bacterium linked to stomach ulcers and gastric cancer. Third party researchers complain that the company's decision to keep this information secret impedes their efforts to develop drugs and vaccines. The company claims a commercial benefit in non-disclosure and the third-party scientists claim a public benefit of disclosure.

## **Information that the public interest demands be kept secret**

All governments have certain information which is in the public interest to keep secret. Matters affecting national security are obvious examples. [That said, a range of cases have demonstrated over the years that executive claims of privilege on such grounds often fail the test of external review. Perhaps these cases indicate that the controllers of such information need to devise new criteria and processes for distinguishing between what information really needs to be protected and that which is merely convenient to withhold.]

## **Information that the public interest demands be accessible**

Irrespective of the commercial interests in maintaining the secrecy of certain information, there are many examples where the public benefit of access is deemed to outweigh the private advantages of privacy, and thus secrecy.

### **(a) Example 1: United States Government Attitude To Encryption**

The well-known "clipper-chip" controversy arises from an application of this balancing of public and private interests in the digital environment. Whatever the rights and wrongs of that argument may be, it is an example of the State, in an assertion of the public interest, demanding access to otherwise completely private, secret information - namely, encrypted digital communications.

### **(b) Example 2: Statutory Licences**

Other variants of the public interest principle, seek to promote access but do not affect secrecy or privacy. For example, where the public interest demands that access to works be assured,

copyright legislation contains exceptions to the subsistence of copyright [eg. the exception relating to works of artistic craftsmanship permanently situated in a public place] and exceptions to the exclusive rights normally enjoyed by a copyright owner: [eg. the statutory mechanical reproduction licence relating to musical works; the educational copying of literary works and audio-visual programs.]

(c) Example 3. Public Access To Information As To The Law

Yet another example of the operation of the public interest of disclosure is the recent initiative of the Law Foundation of New South Wales. The Foundation has established a comprehensive legal information service on the Internet. Known as "Foundation Law", this web site provides access to the full text of State, Territory and Federal Government legislation and regulations; reported and unreported judicial decisions of the High Court, all federal courts and tribunals, state Supreme Courts and other state courts; daily court lists; information from the Commonwealth and State parliaments such as bills, digests, and weekly Hansard; document exchange and e-mail etc. (See Foundation Law's home page at <<http://www.fl.org.au>>).

It is an extraordinarily innovative example of how the public interest can be served by re-examining the traditional methods of information distribution and access. This material was all previously available to the public but often only through expensive proprietary repackagers (the legal publishing companies) or by means of inefficient labour intensive, searching procedures.

In an era in which the legal profession is under pressure to reduce the cost of legal services (that being one of the relevant public interests), this quiet revolution in the provision of access to legal information would not have been possible without the technological developments of the last two years. It is an example of how digital technology is changing the means of access to information and therefore its accessibility, its cost, its value and its form.

There is presently no charge for any of the information provided on Foundation Law. This is appropriate given the importance that we, as a society, place on public access to justice, the courts, and legal information.

That said, where the balancing of interests permit, this information service might distinguish between free access and paid access to certain materials. For example, assume that the Law Society wished to assist small law firms by establishing a base of precedent documents. Practitioners could place on the data base selected precedents that they have developed and nominate a charge for using that document. A portion of that fee could be retained by the administrator to pay for the system and the remainder could be paid through to the owner of the information. This would be a system in which the private commercial interest would benefit from leverage and the public interest would benefit from the promotion of access.

(This is itself an example of how technology affects our ability to deal with information: two years ago, the systems for conducting commerce on the Internet were notoriously insecure. Now there are a number of systems capable of administering such digital transactions. Although none of these technologies have yet established themselves as the reliable industry standard, the existing technologies are certainly already sufficiently secure for these purposes.)

## **Evaluation of Information**

The danger of the global networking of information that accompanies the continuing development of the Internet and other on-line communication technologies is that these technologies promote information availability but not necessarily the value of its content. No corporate information is in itself valuable and availability is no asset without relevant quality content.

There are three stages at which information evaluation is important: First, when the decision is made by the owner to make certain information available; secondly, when the decision is made by the user to access a particular piece of information; and thirdly, the dormant stage in between, (for storage is one of the great expenses of running any private or public enterprise).

## **Selection criteria for determining third party access**

Any process of administering access to information must start with an evaluation of the information by the owner. This must be done according to guidelines and procedures that have been tailored to the circumstances and characteristics of the individual corporation or government department and according to the characteristics of the particular item of information.

Whatever the technological nature of the storage and administration system, the information must be accurately categorised and processed. It is this classification task that requires a high degree of care and skill. Whilst there are efforts being made to develop artificial intelligence agents and decision support systems (DSSs) to undertake some of this task, it is perhaps a process that may not lend itself to computerisation or formulae. Perhaps the final decision, where any sensitivity is involved, is a matter, which inevitably requires the benefit of human judgment. In some ways, it is comforting to think so - even if that judgment is assisted by software.

One thing is certain: Given the risk of information overload that results from modern information technologies, the commercial value of information is established and maintained by the "value-added" such as classification, organisation and the ease and attractiveness of access and navigation. Volume alone, is not significant.

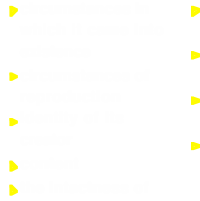
## **The Quality Of Confidentiality Or Secrecy**

Although this does not accord with our traditional approach to information risk management, there is probably no such thing as inherently confidential or secret information. The value of these qualities may vary with:

- (a) the circumstances in which it came into existence [such as board or cabinet minutes];
- (b) the difficulty or expense of its genesis [such as the results of long-term original high tech research];
- (c) the circumstances in which it is reproduced;
- (d) the age of the information [for time erodes the rationale for secrecy];
- (e) the identity of the creator of the information;

- (f) the identity of the receiver of the information;
- (g) the content of the information;
- (h) whether the disclosure of the information may reveal secondary information which is confidential or secret [such as the identity of a source or the so-called “train of inquiry” cases]; and
- (i) whether the confidentiality of that content is still intact.

#### SECURITY/CONFIDENTIALITY EVALUATION FACTORS



Assuming that these factors result in conferring on information a range of importance and value, an access provider will need to structure its access criteria so as to reflect that hierarchy. The difficulty with all assessments of the need for and value of confidentiality or secrecy is that there can be no valid **objective** criteria for such decisions. The decision, although it may be subject to decision-making guidelines, must inevitably be **subjective**: the decision of an individual (or a small group of individuals) who are applying their own interpretations and valuations on both the information and the circumstances affecting its importance.

Indeed, even when the owner or possessor of information chooses not to reveal information because of perceived confidentiality or secrecy, many judicial decisions now show that the issue of whether or not information is kept confidential or secret is quite separate from the issue of whether the information should be disclosed. The former, tends to be a decision taken by the possessor or owner of the information; one based on the decision-maker's subjective (and sometimes self-interested) evaluation. On the other hand, judicial decisions as to whether such information should be revealed, are usually achieved by an external evaluation of the diverse competing public interests.

The courts have extensively canvassed this tension between the interests of disclosure and non-disclosure and it is not the purpose of this paper to survey that discussion. The point to be drawn from the judicial commentary is a short one: confidentiality and secrecy are important but highly subjective and ephemeral concepts. What is significant to me, may not be to you; what is confidential today, may not be worth protecting tomorrow; what is worthy of secrecy when uttered by you, may have had no significance when uttered by me.

#### ***The Valuation Of Corporate Information***

Just as the quality of confidentiality or secrecy can vary, so too can the value of the information. Much of the perceived benefit of warehousing corporate information is illusory. Much of it will go out of date before it is used again by the organisation that created it.

Whereas the price is something determined by the seller of access to the information, the value is necessarily determined by the customer. What the access provider believes to be of extraordinary value may have virtually no commercial value to third parties. The contrary is also true. This is one of the great dilemmas of setting prices in a market, which is both competitive [for the sale of information is certainly competitive] and yet deals with a commodity the value of which is determined on a case-by-case basis by the purchaser.

In an information environment of potentially huge volumes, it may simply be impracticable to determine who is going to want access, the purpose for which they might seek that access or the benefit that will flow to them from that access. Unless you know or can make assumptions as to this sort of information, it is impossible to cost information according to its perceived customer value. So what is the answer?

Existing valuation strategies are unsatisfactory: The price may be one that reflects the value of the information:

- (a) to its owner;
- (b) to the buyer, as perceived by the owner;
- (c) to the buyer, as demonstrated to the owner through market experience.

The first is objective but irrelevant; the second is subjective and unreliable, and the third is often impracticable (for the volume of data is enormous but its shelf-life is often short).

These were approaches devised in relation to goods and services rather than the more ephemeral subject matter that is information. Furthermore, most strategies were developed in an age when spring-back folders were new technologies of information management.

### **Security: A Core Issue In Information Access Management**

One of the fundamental aspects of risk management is the development of strategies to ensure the ability of authorised users to access corporate information. Whilst software developers might say that this is a fundamental characteristic of database management systems, mere software programs can not achieve the task by themselves. Indeed we should ask whether we have been over-reliant on technology to provide for our security needs.

Should not security strategies be multi-disciplinary? The management and psychology of security is as important as the technology. Scientists may strive to provide better and better firewalls against hackers but security breaches are probably more commonly permitted by the failure of management than by the failure of technology. No security system is safe from the computer operator who writes an access code on a yellow Post-it note and sticks it on the side of his computer. No company's system is safe when the access code is the name of the company.

It is not the intention of this paper to discuss the elements of any basic IT security regime however; any system of information commerce must be able to ensure that:

- (a) the stored information is authentic;

- (b) unauthorised modification of it is prevented;
- (c) the owner is authorised to possess and reproduce the information;
- (d) user access is authorised;
- (e) the information is available to authorised users;
- (f) the information is communicated unaltered;
- (g) completion of the transaction is duly verified; and in some cases,
- (h) the transaction is confidential.

Unless these matters are attended to by the information provider, no networked commercial system is useful.

### **To Be Valuable It Must Be Found**

In a digital information world, where anybody can be an author and distributor, the greatest challenge to information value is how to tell those who may be interested in your information (a) that it is available and (b) how to find it, in the midst of the cacophony of available digital material that is competing for attention.

Again the answers will be multi-disciplinary. Some components will be technological and others will be more organisational. For example, the popularity of the Internet has increased as browser technology has developed. This is a technological solution to overcome a normal, human, psychological resistance. The more friendly the interface between the human and the bits, the more accessible are the bits.

Other solutions are organisational. They are driven by marketing. An example of this is found in the proprietary on-line services such as e-World, America Online, On Australia, Prodigy or CompuServe. In subscribing to such a service one is buying the advantage of access to an organised information filter. Perhaps the success of these proprietary services is an admission that in a world in which the volume of information is virtually infinite, speed and simplicity of access to relevant information may be more important than breadth of coverage.

[The corporate advantage of these organisational solutions is again illustrated by Foundation Law. This service may become the dominant Internet site relating to legal services in Australia (for there is no commercial advantage in trying to compete with a free service that is also comprehensive). Carefully developed, this site will become the focus of both free and fee-based Australian legal information services. There is no reason why it should not contain hypertext links to other relevant sites that its administrator deems useful. What lawyer is going to start the search for information anywhere else?]

In brief, the immediate challenge is to develop new marketing strategies and ever better new navigation tools. Potential clients have to know that the information exists and it must be easy to find.

## New Technologies Reveal New Risks

Although there might be no reliable standard by which the merit of any **class** claim for secrecy or confidentiality can be assessed, ambit claims for confidentiality and secrecy were understandable when information was written on paper, organised in manilla folders and stored in filing cabinets. In most countries this is changing fast.

Computing and in particular database management systems are helping us make those decisions on an individual basis, thus allowing more sophisticated degrees of disclosure and access than ever before.

We have seen the development of hierarchical databases, relational databases and multi-dimensional databases. Whilst each brings new advantages to dealing with information, each brings new difficulties. For example, multi-dimensional databases, as their name implies, can store data in any number of dimensions and have the ability to summarise, consolidate and relate information.

Take the facility to relate and consolidate. So-called **upward consolidation** may well be in the public interest whereas so-called **drill-down** capacities may result in dangerous breaches of civil liberties. For example, if you relate and consolidate information as to health, property ownership, financial, and buying patterns from the profiles of 10,000 individuals, you may have research findings that provide Government departments with a fantastically sophisticated planning tool. On the other hand, a multi-dimensional database permits downward drilling, whereby you can start with the information that is descriptive of a group and end up revealing very confidential information as to the individuals making up that group, assumptions that may, because of the relational and interpretive qualities of the technology, go much further than the provider of the primary information ever contemplated.

This is at the heart of the debate in the US concerning the extraordinary "LandView TM 11" information retrieval system. This is a set of 11 CD-Roms, which includes EPA and Census information providing "demographic and economic data, including statistics on race, age and income, and displays of networks of roads, rivers, railroads and landmarks. It can display boundaries for states, counties, congressional districts, metropolitan statistical areas, census tracts, Indian reservations, and Alaska Native lands. There are excerpts from five of EPA's major databases, representing many of EPA's primary activities. The system includes desktop mapping capabilities, and the user's own databases can be imported into the system and displayed if geographically coded" ["Blast", The Bulletin of Law/Science & Technology, American Bar Association, October 1995, pg 10]. This is but one way of Government departments providing public access to "right to know" information and, at the same time, selling the information for \$95 per disc or \$795 for the set.

Intelligent technology will be an essential tool in resolving the problem of granting and administering large-scale access to information. However, information risk management demands that the technology of selection and administration of information be subject to an examination that is just as rigorous as that imposed on the technology of access.

## IP Control And Prevention Of Abuse

Over the last 100 years, intellectual property has been fundamental to any analysis of the value of information. At last we have an international system based on treaty memberships, which is providing large-scale, albeit imperfect, protection for intellectual property. Such is the value of this asset that we have seen it as one of the recent battleground of inter-government economic negotiations.

The value of intellectual property is rooted in the ownership control conferred by copyright's international system of exclusive rights. For this reason, the globalisation of information communication technologies is the greatest threat ever posed to intellectual property-based value. Once information is released on-line, there are, as yet, no completely satisfactory systems available to assist information owners to:

- (a) track the reproduction path taken by their copyright material;
- (b) ensure the on-going integrity of the content of that material;
- (c) promote the accurate attribution of authorship;
- (d) withdraw information which has been compromised or otherwise requires retraction; and
- (e) ensure that their economic interests are protected and promoted by a system of remuneration for the digital reproduction of their information asset.

There is, of course, considerable work being done in these areas but until industry standards evolve, most of these attempts must necessarily be piecemeal. Bodies such as the OECD have an important role in facilitating and promoting the development and establishment of appropriate international standards thus ensuring that consideration is given to long term public interest rather than merely short term commercial interest.

## The Ownership Of Digital Information

One of the interesting issues that is fundamental to the control and exploitation of corporate information is that of **ownership**. With information storage and communication technology changing from being paper-based to being digital, the traditional analyses by which we determine ownership of information has been challenged.

If the method by which information is communicated can affect the meaning of the information and thus the very information itself, how do technologies affect ownership? Are different principles applicable to an author of a poem using English language and the author of a work in binary code? Should we treat the author of a poem differently from the author of a database management system? Should we treat the author of a novel who publishes in volume form differently from the author of a novel who publishes on the Internet? The "copyright is dead" school of digital thinking is predicated on a belief that digitisation necessarily and profoundly affects the legal relationship of the author and the user of the information.

The significance of this is that these attitudinal changes are occurring within the digital community without sufficient thought leadership from Government.

Issues of ownership are important if we are to maximise the value of corporate information. They are fundamental to any analysis of the right to control information and the right to commercially exploit it.

The difficulty is whether, in a global market, any national government can see any advantage in tackling the issue. My belief is that Governments must be a participant, indeed **leaders** in the public debate. The global nature of information communication systems and markets is such that meaningful legislative control will only be achievable by constructing an international web of reciprocal treaties. This has been the method of ensuring the international protection of intellectual property in the world of atom-based material and it is the only way of protecting bit-based information.

Government must be a leader in this debate so that it has the opportunity of being an active participant in the formulation of public policy rather than merely leaving the solution to those who would see copyright consigned to the scrap heap along with the music box and the player piano.

### **Legal Issues Are Management Issues**

As long ago as 1987 the US National Research Council Report stated that effective management of technology:

“links engineering, science and management disciplines to plan, develop and implement technological capabilities to shape and accomplish the strategic and operational objectives of an organisation.”

To this, must be added one further element: the Law. In the world of convergence and the global access to information, the Law is one of the key tools with which we permit, encourage, structure and enforce those strategic and operational objectives.

There has been a plethora of conferences dealing with copyright, defamation and pornography on the Internet and on-line services. It is not my function to replough those fields today. Much more important in a commercial environment are the issues of negligent mis-statement, professional liability, jurisdiction, privacy, ethical standards, and the attendant social, political and financial effects that can flow from such issues.

These are not issues that defy traditional legal analysis merely because they have application in the cyber world. Just as each nation must form its own views and its own responses to these issues, each corporate owner of information must, likewise, consider them in formulating its own information strategy. Rather than taking a negative view and treating these matters as potential hurdles, a creative, management-oriented view is required. One must **manage** the legal problems that arise from the technology.

Those who are successful in management, recognise the most likely pitfalls and develop strategies to manage and minimise those risks. They implement administrative guidelines, behaviour codes, corporate training programs, standard terms of doing business, standard contracts, standard releases, and so on. Just for brevity's sake, let's call these various risk minimisation and effectiveness enhancing devices, “**risk management protocols**”.

The test thus becomes: How do we use our existing skills and advantages so that they provide similar benefits in the new environment? The rationale is simple enough: The Law inhibits certain behaviours and encourages others.

This intent is based on social, ethical, economic or political rationales that rarely change with a mere change in the medium of expression or distribution. Cyber-space is just another medium of social and commercial relationship.

Similarly, as copyright law faces new pressures from digitisation and global access technologies, corporate information strategies will be best achieved by using management skills and technological expertise, in conjunction with traditional legal analysis and advice. Many of the legal problems can be engineered away; others can be managed away. Thus, in implementing the decision to allow third party access to corporate information, the process of developing the “risk management protocols” will require intensive corporate introspection:

- What is your strategic objective in granting third party access to corporate information?
- What types of information will you make available and on what terms?
- How will you select that information be selected? On what criteria?
- Do you have the right to grant third party access to that information?
- What level of access do you want to license to third parties?
- What use do you want them to be able to make of the information obtained from this access?
- What design factors need to be built into the information to promote your aims and minimise the attendant dangers?
- What hardware and software assistance can be built in?
- What human resources are available internally/must be hired/must be trained/must be supervised, to effectively implement and administer the access program?
- What will be the terms of the contractual relationship between the owner of the information and the client seeking access?
- How will that relationship be achieved, documented, supervised and enforced?

This is an example of **managing** major legal problems by acknowledging the risks and adopting non-legalistic methods of meeting those risks.

## How Do We Do It?

Practicability is often the nemesis of what was otherwise an apparently good idea. Most organisations do not have the human or financial resources to plan, let alone implement, such a radical rethinking of their attitude to their corporate information.

### 1. Planning

If we do believe that there is value to our corporate community, our national community, our global community, in facilitating the controlled release of this store of human intellect, I suggest that the research should be undertaken by a team containing multi-disciplinary expertise. This is not just a challenge for computer science and information technology. It is not just a management problem. It is not just an economic issue. It is not just a series of legal problems. It is not just an ethical dilemma. The challenge of information leverage is multi-disciplinary and the approach taken to its resolution must, similarly, be multi-disciplinary.

## 2. Implementation

It is a brave person who suggests implementation models before undertaking the underlying research. That said, one point can be made: Some organisations will reject the basic proposition of this paper on the basis that they will never have the resources to implement and maintain adequate access and dissemination systems. The answer, I suspect, is in outsourcing. There is no reason why many of the elements of the business of information leverage should not be outsourced. For example, while information selection and valuation might be kept in-house, the organisation may choose to outsource the data warehousing, security, administration, dissemination and accounting functions. The “information administration and repackaging industry” will be one of the great businesses of the future.

## Conclusion

Information, has no intrinsic value. Its value, like beauty, is in the eye of the beholder. Similarly, there is no inherent public interest or private advantage in access to information. That said, information organisation and communication technologies now permit a quantity and quality of information that must change our management approach to this asset.

The challenge now facing the information and technology rich organisations is to develop elegant, effective, risk management protocols to maximise the benefits and minimise the risks that attend the handling, storage, classification, accessing and application of information. Those that do develop these templates and guidelines will be providing a service of the greatest public benefit.

If information is the embodiment of human endeavour and intellect, it is in our unquestionable community, corporate and government interest, to facilitate and promote sensible access to the riches of corporate information.