

Government Service Delivery in Cyber-world:

Practical Risk Management

GOVT. OF WESTERN AUSTRALIA

23rd April 1996

by

Professor Shane Simpson

Director

TECHNOLOGY RISK MANAGEMENT CENTRE

Many government departments are already using the Internet as a tool of product and service delivery. Many are at least considering it. Even more feel guilty because they think that they should be considering it.

Western Australia is one of the most advanced of the States in seeking out and applying advanced applications of IT&T technology to fulfil the delivery of government services. That said, as this audience is largely made up of people who are in large part responsible for Western Australia's IT&T position of leadership, I am somewhat hesitant to stand before you and tell you how to suck the IT&T egg. In this room there is considerable experience in designing, implementing and reviewing strategies for the application of IT&T to government programs. My contribution this morning is deliberately "low intensity". Let me explain.

Those of us who are used to using technology can all too easily forget that many of those who are responsible for the management of the delivery of government programs, do not treat computers as their friends. Even the term IT&T is one that is divisive: one that separates "us" and "them". This morning I want to look at just part of the process by which the "them" might feel more comfortable in applying innovative IT&T solutions to government service initiatives.

Today I am also going to probably make myself unpopular by using the term "business" to describe the various functions of government departments and agencies that can be delivered by the Internet and on-line services. It is a crude piece of shorthand and by it; I do not mean to imply that the department should necessarily be charging for the service or product. That is an argument for another time.

Anonymity, Anarchy and the Rule of Law

When implementing any government function, one of the basic elements of any effective risk management strategy is to consider the relationship of the function, and the process whereby that function is to be delivered, to the Law.

A legal hiccup can result in political death and so must be avoided.

Part of the problem we face is that there is a body of thought, which suggests that the Laws of the atom-based world do not apply to the bit-based world. At best, most of these arguments tend to be based on a philosophical position of the author rather than any analysis of the Law. At worst such arguments are just column space.

The proponents of such beliefs are dangerous to those charged with risk management. They are not basing their behaviour on the same philosophical construct as that underlying the plan. Without wishing to over-react to this, may I suggest that this is something that you must look to in personnel selection and on-going training for if a member of your IT&T implementation team is working according to a different paradigm, you have a problem.

Our purpose this morning is not to discuss ways of dealing with 'paradigm clash", so let us merely identify the need for consistency within the implementation team and eventually, those charged with its day to day operation. Quite simply, we must not let an illusion of digital anonymity trap us into believing that cyber-space is not just another part of our community. Laws apply now; laws will continue to apply.

After hundreds of years of tension between the Law and technological development, one would think that society is used to (indeed prefers) the fact that the Law is always a follower rather than a leader. The Law took centuries to deal with the consequences of the printing press; it took decades to come to terms with the phonograph and many years to develop coherent laws relating to the photocopier (and some would say that it hasn't yet achieved them). The Internet presents bigger legislative problems than all of these, so I would not expect that we'll solve them in the next few months. Decades perhaps.

At the moment there are few laws and international treaties, which specifically cover cyber-space, but the Law is not going to ignore cyber-space or the Net. Society cannot afford to allow that. Such Laws will increase.

Ten years ago there were no court decisions about it; now there are. Already in Western Australia you have had one of the world's first defamation cases involving publication of a defamatory statement on the Net. Except for the novelty of the means of publication, it wasn't a very interesting case; it was really quite mundane! The law simply treated the statements in the same way as it would any other.

Similarly, we are now getting considerable activity from the press officers of various government Ministers who have decided that it is a priority to outlaw pornography on the Net. Is there anything to suggest that they will be any more successful than they were in controlling pornography in print? But let's not get into that argument. Let's accept that there is a benefit in being seen to be doing something even if that something is ineffective. We will get the cyber-porn laws that we either deserve or that others believe we deserve.

Issues such as defamation or pornography will have little influence on business. Yet it is use of the net and on-line services by business that is going to be the next business revolution. It will not only create new businesses; it will change the way existing businesses are controlled and delivered. This is where significant legislative influences will be felt. Governments will respond to the demonstrated needs of government and corporate users of the Net and on- line services.

In the meantime, we are regularly told of the many legal difficulties and restrictions related to doing business on the Internet: We are familiar with the copyright problems, defamation difficulties, security imperfections. We also are probably reconciled that it is going to take some years before legislatures develop adequate responses to many of these problems and that it will be a similarly distant time before R&D produces effective technological responses to such problems.

That said, rather than taking a negative view and treating these matters as potential hurdles, I am going to suggest that we take a creative, management-oriented view. Part of the problem is that the majority of a government's managers are not hugely computer literate let alone computer wise. I realise that today's audience is almost uniquely experienced and competent in the use of IT in the delivery of government business - but you are the vanguard. What I am presenting this morning is an approach which may assist people manage the legal problems that arise from the technology without their being drowned in by the resistance that flows from the insecurity of ignorance or unfamiliarity.

If we are successful in the delivery of government business (as it has traditionally operated) it is because we know the most likely pitfalls and have developed strategies to manage and minimise those risks. We have implemented administration 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 protocols".

If you already have risk protocols in place, it is likely that the need for these and the principles behind them, will remain relevant in the electronic environment. Cyber-space is just another medium of relationship. Accordingly, liability issues are no less important when using the Net than when using letters, newspapers, magazines, radio, television or billboards.

The reason 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.

For example, if copyright is one way that society financially rewards creative risk-taking, that rationale is the same whether an unauthorised reproduction is by means of the Internet or a bootleg record. Similarly, if there is a public interest in ensuring that an advertisement in a newspaper is not misleading or deceptive, that public interest is no less when the medium of expression is the Internet.

The test thus becomes: How do we use our existing skills and advantages so that they provide their proven benefits in the new environment?

After all, what your department or agency needs to achieve is the advantage of doing business in a new medium without suffering the disadvantages that can flow from inexperience in that medium. I would suggest that if we are to succeed in using the new technologies to enhance the effectiveness of government programs, we must make that process as ordinary as possible; by relating as much of that process as practicable, to that which is already familiar.

I suggest that the answer lies in a simple five-step process: one that uses no magic words:

- MANAGING THE RISKS
- OF LIABILITY
- REVIEW
- AMEND
- DEVELOP
- IMPLEMENT
- SUPERVISE

STEP ONE - REVIEW:

Review your existing procedures.

The prudently managed department or agency will already have developed risk management protocols for the existing means of carrying on its business. The expansion or evolution of an existing business into this new medium will probably mean that the existing risk protocols will be relevant - but inadequate. Let's take a couple of examples:

(i) Intellectual Property Protocols

John Perry Barlow would have us all believing that the Internet has either killed copyright or at least is causing it to suffer a long and grotesque death. As I have already alluded to, the prudent risk manager cannot allow this polemic affect his or her judgment.

Given the enormity of current and on-going investment in Intellectual Property, there is little likelihood that the "Copyright is dead on the Internet" line of argument will win through. Intellectual Property makes such a major contribution to so many corporate balance sheets that merely engaging in the rhetoric of anti-copyright nihilism is not the answer.

To explore what may be the answer, is not the purpose of this paper. However we can say with certainty that few companies are or will be prepared to give away their intellectual property assets.

Many however, may be prepared to share them or trade them in return for some reciprocated benefit. It is a matter of devising the mutuality of benefit and establishing the systems and procedures which will ensure that mutuality. The Internet is going to force us to develop and consider new ways of exploiting the value of our intellectual property.

For example, if your department advertises its products or services using traditional media, you will already have a procedure for ensuring that the words, art, film clips, music, used in those advertisements are free of copyright problems. To this end, if the work is done "in-house", reasonably detailed procedures should already exist to ensure that a nominated person is responsible for obtaining the copyright permissions needed or perhaps, that all designs used are wholly created in-house and thus, no copyright clearances are necessary.

If you are going to use the Internet for similar purposes, you must review those procedures to ensure that those existing procedures are relevant to and effective for the new medium. After all, the need remains the same: the laws of copyright applying to artistic works, designs, film and music, apply to uses in cyber-space just as they do to column-space. Some rules might be slightly different; some will remain unchanged; but rules there will be.

Let's apply this copyright theme to the use of on-line corporate information. A number of corporations and government departments, at considerable expense, maintain many databases that are presently designed for use by their employees. There is an increasing pressure from the clients of these corporations, to be given on-line access to this corporate information. In earlier years, the reaction to such a request would have been astonishment, followed by haughty rejection. The information would have been seen as part of that mystical body of dark secrets that were hoarded by its owner. That was part of its secret "know-how".

Nowadays, the mood has changed and we are all more attracted to doing business with those who share rather than those who play the old boys' game of "information as a power tool". As soon as we provide third parties with access to corporate information, we need to have an even tighter control of our copyright regime: (the wider the publication, the greater the potential damages). Accordingly, if we are going to give clients Internet or on-line access to information, we must review radically our existing protocols:

- What level of access do we want to grant to third parties?
- What use do we want them to be able to make of the data obtained from this access?
- What design factors need to be built into the database to promote our aims and minimise the attendant dangers?
- What hardware and software assistance can be built in?

By asking these sorts of question, you are handling a major intellectual property issue by acknowledging the risks and adopting non-legalistic methods of meeting those risks. What you are doing is pro-actively managing a major corporate asset rather than merely waiting for something negative to happen.

(ii) The Need to Take A Wide View

In reviewing potential liability exposures, do not be blinkered. Often clients are so focussed on one potential risk that they completely ignore another risk - one that can be even more dangerous.

For example, I have just been discussing third party access to corporate information as a copyright issue. It could also raise a number of others that are potentially more dangerous - such as professional liability and negligent misstatement. Put simply, you might be liable for errors contained in the information resource if the third parties rely on the defective data to their detriment. What a pity if you were to build beautiful risk protocols that protected your intellectual property asset but left yourself exposed to another, even more dangerous risk.

(iii) Cyber-documentation

Another likely area of review is the way that you document transactions. For example, as you know, for a contract to be enforceable you must be able to show that there has been an offer and that it has been accepted. It is fundamental to your business that the terms of your offer are controlled.

When this is happening in a traditional atom-based environment, that process is difficult enough but on the Net, you would be wise to audit the formal process by which you intend to bind your clients so that you are absolutely sure that you are achieving your corporate intention. We are used to having our contracts negotiated, drafted and reviewed by lawyers and we are familiar with the benefits of having this done. We are not so familiar with having our cyber-transactions similarly vetted. Yet the need is no less.

For example, you may have already developed standard contracts and standard forms which were developed for non-electronic purposes. Review them to ensure that they are still relevant and have suitably expert legal advisers check them over to ensure that they legally achieve your business purposes. They will almost certainly need amendment.

Also review all releases or licences or permissions which were drafted for use in non-electronic media. They will almost certainly not be adequate for the digital age. Similarly, most exclusion clauses in agreements for the provision of goods or services will need to be varied. The courts take a restrictive interpretation of exclusion clauses and they must be very specific and precise.

These are not daunting processes. Treat the investigations required by the new medium merely as extensions of our existing, familiar risk management procedures.

(iv) Jurisdiction

The Internet is not concerned with the issues of States' Rights. It does not see transactional control as either a state or federal issue. As we are now very aware, the international nature of Internet transactions means that in a contract dispute, it can be virtually impossible to determine,

- in which country the parties are living,
- where the contract is being entered, or indeed,
- where the contract is being breached.

It is therefore difficult to determine which state's or country's laws apply. All standard contractual terms must be amended so that this important issue is clearly defined. It is not impossible, but the consequences of not doing it can be disastrous. This is an important issue for all governments which are using IT&T to provide its citizens with access to corporate information.

Is it significant if some of the users are not citizens of that government? Is the government prepared to provide such services to the world at large? Is it prepared to incur the same levels of liability to non-citizens as it is to its own citizens? What are the boundaries of responsibility? How are they to be defined? How are they to be maintained?

(v) Employment Issues

The adoption of new IT&T procedures can even affect very simple employment liability issues: Let's assume that instead of giving employees a pay slip an agency decides to save a lot of money by providing employees with e-mail notification, thus saving a lot of administration and a lot of trees.

As some employers have recently found, this may be the cause of considerable staff revolt because standard Microsoft e-mail does not guarantee the privacy, confidentiality or sensitivity of data. Given the possibility that such material may be read, changed or copied, is this an appropriate use of the technology? Is there a better way of doing it?

(vi) Confidentiality and Responsible Levels of Security

Extend this example to a larger issue. If an agency is using the Internet or an Intranet to communicate information which is commercial in confidence, has it adopted a software encryption program which sufficiently protects the security of that data? If not, it is either being irresponsible with its core business information or being irresponsible towards its client's business information.

Either way, it is exposing its business to potential damage and loss. The more important the information, the more disastrous is the effect of any security breach; the greater is the effect on the organisation, (the more damaging are the political ramifications), and the greater the priority of this management issue.

(vii) Defamation

As already mentioned, we already know that defamatory statements delivered via the Internet are just as defamatory (and expensive) as similar statements made in a newspaper. If departmental staff is to have access to the Net which permits them to voice potentially defamatory views, we must look at the department's existing protocols to see that they are still relevant to a digital system of distribution. Bad enough for a university to have one of its employees found liable of defamation; worse still for an employee to expose the government to such expense and embarrassment.

I would suggest that there would be no faster way of impeding government initiatives in the use of IT&T than to be blamed, perhaps unfairly, for such embarrassment.

Newspapers have highly developed systems for having potentially defamatory material proofed by their lawyers before an article goes to press. These systems are cumbersome and difficult enough when the publication and distribution mechanism is physical, but they become vastly more difficult when those mechanisms are digital.

What does your department or agency have in place? Have these mechanisms been amended to take into account the extraordinary effect of making every Internet user a potential publisher of defamatory or injurious statements - for which injuries the employer can be held liable?

(vii) Conclusion

So, the first principle is REVIEW your existing liability management protocols, to recognise their importance and acknowledge the rationales behind them. When you are tackling a new environment such as the Internet, it is unlikely that the basic rationale behind the protocols will have much changed. Most of them will still be relevant, but "best practice" demands that you subject your risk protocols to continuous review and criticism.

STEP TWO - AMEND

After you have reviewed existing risk management protocols, you must amend.

A thorough review process generally provides many of the answers as to what needs amending and how best those amendments might be made.

Amending risk management protocols demands a range of expertise. Some of the problems can be managed away; some can be engineered away and some can be dealt with by legal mechanisms. Because solutions are multi-disciplinary, so must be the team that devises them. If it is not, it may not sufficiently identify the problem or may not find the most simple, effective solution. The task requires teamwork; not just the usual collection of individuals with separate expertises working under the label of a team.

STEP THREE - DEVELOP:

Doing business in cyberspace requires a degree of humility and a capacity for on-going learning. None of us are truly expert, no matter what our promotional brochures may tell the world. It is a brave person who purports to be aware of all of the latest developments because, every day, the landscape changes.

Accordingly, we must be continually prepared to develop our procedures; to be self-critical not self-congratulatory. What worked for us last week will not necessarily be "best practice" next week. We must always seek to develop and improve the procedures we use to transact our business on the Net. We often concentrate on making our Web Site more attractive, on making it fun, zany, cool and easy to use but forget that underneath that friendly attractive customer inter-face there is a hard-edge purpose.

Just as we keep working on the user-friendly aspects of our relationship with our cyber-public we must spend similar attention and resources on ensuring that the social, commercial and legal imperatives of our business are well protected. These will mean that we must invest the time, effort and resources on developing the new risk management protocols; those that weren't really necessary in the former, atom-based environment.

Let's use some examples that concern that essence of any successful enterprise: quality communication with our clients. As you are aware:

- There is little guarantee that a message on the Internet has been (a) received, or (b) received in the form it was sent;
- Similarly in a world in which time is frequently of the essence, can you tell when a communication was actually sent or when it was actually received?
- Can you even prove who sent the message?

If you can't be sure who you are dealing with, what they are saying, when it was said, or even whether you are communicating at all, is the long-term foundation of your enterprise on the Net fundamentally flawed?

Ask any in-house legal counsel how many contract problems arise from poor communication levels and you will find that it is one of the most important factors in deals that go bad; in expectations that are not met. The financial, legal, social and political consequences can be considerable.

STEP FOUR - IMPLEMENT:

All the other steps were about identifying the threats and designing your administrative firewalls to protect you from liability. This step is about actually building that firewall.

This is really a management issue. There is no point in developing risk management protocols if you don't have a system for implementing them. There is no substitute for developing clear, fully articulated implementation procedures and ensuring a high-level of staff training so that all staff members are absolutely clear as to their responsibilities.

Again, this might seem obvious to an audience such you, but it is my experience that, all too often, the implementation issues are delegated to one or two people - who are then promptly marginalised within the organisation. We all like to leave responsibility to others but it is important that we find ways of having all of the staff aware of the risk management protocols and, more than that, accept a degree of responsibility for their effectiveness.

Implementation is an exercise of authority and those charged with implementing change must be given sufficient real power to accomplish that task. Are those persons going to be from inside or outside the immediate organisation? With whom should they confer? To whom should they answer? How is their role to be introduced to the rest of the workers?

It must be recognised that change is a two way street. Just as it affects the department and its workers, it affects the public (or other customers of government's business). Who is responsible for implementing the process of change within the client group? There is no point developing on-line Government Information Kiosks unless the public knows that the service exists, finds it comfortable and easy to use, finds that the information is in a form that is appropriate to their needs and is available for a cost that they feel they can afford.

STEP FIVE - SUPERVISE:

Supervision is that ongoing responsibility of management to ensure that the processes of Review, Amendment, Development and Implementation are an organic feature of the administration of the agency.

Not only is this a basic characteristic of any efficient management regime; it is also a basic feature of the government department's legal, economic, social and political regime. It is the only way that you can be sure that the transactions and communications that you undertake will have the legal effect that you intend: maximising the opportunities and minimising the attendant threats.

CONCLUSION- The Place of the Law and the Process of Change

If change is a fundamental characteristic of the medium it is hardly surprising that effective use requires new approaches to familiar issues.

In this lecture I have used the Law as a metaphor for the various strategic elements that we must consider when managing innovation or technological change. Others can discuss the technology strategy, process strategy, marketing strategy and human resources strategy. They are all essential to the development and implementation of effective risk management protocols

None of this innovation management stuff is in itself revolutionary. The revolution is happening elsewhere. The Internet has created a new way of communicating. The importance of this is that when we change the way we communicate:

- (i) a new social environment is created;
- (ii) new economies are created; and
- (iii) organisations are changed both in their internal and external function.

Why is this? Because information is affected by the technology by which it is communicated.

The means of communication affects the way we perceive the information being communicated and thus, inevitably, affects the information itself.

It also affects the way we perceive the person with whom we are communicating and the way that we are perceived. It is essential that government agencies using this new medium appreciate the subtlety and power of this.

SIMPSONS

SIMPSONS SOLICITORS
Level 2, Pier 8/9 23 Hickson Road Millers Point NSW 2000 Sydney
Phone +61 2 8014 5050 Fax +61 2 8014 5060
www.simpsons.com.au

On the Net there is a certain atmosphere of digital anonymity. It is perhaps this characteristic that gives as much strength to the poor as to the rich, makes us blind to the beautiful as well as the ugly, which creates an environment in which there is no hunger or homelessness and responsibilities are only recognised according to the rules of membership of the cyber-club.

One of the great challenges of the provision of government services through the use of IT&T is to humanise that process of engagement for, if that service provision is to be effective, it must maintain the delicate balance between cost effectiveness and the quality of the human experience.

Intellectual
Property.
Entertainment.
Publishing.
Media.
Visual Arts
& Design.
Museums
& Galleries.
Litigation.

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