

A PROPOSAL FOR A NATIONAL GIGAGBIT USERS LICENSE

1. SUMMARY

ROAR Film Pty. Ltd. (ROAR) (www.roarfilm.com.au) is a Tasmanian company specializing in on-line cyber risk education, primarily in the K-12 sector in the United Kingdom, where 41% of English public schools use its products.

Cyber risk is the combination of cyber security, safety and citizenship risk issues, which are closely linked.

These risks will grow as end user bandwidth expands, becomes more mobile and symmetrical and applications arise to take advantage of these features. ROAR is already seeing these trends amongst its customers.

ROAR notes that many cyber risk issues involve externalities where the behavior of one person generates costs for others, often on a large scale. Many of these costs are, for most part, not borne by the agent causing or generating the problem.

These externalities provide a rationale for entities ranging from governments to other organizations, such as schools and firms, to try to prevent such risks, or to contain their costs.

Some cyber risks are only amenable to detection, prevention or control via physical restriction at source. These include, for instance, risks that are hard to detect such as when a computer becomes part of a botnet.

However, it is equally true that many cyber risks can be prevented or mitigated by trying to influence the behavior of end users, which can involve elements such as regulation of behavior, certification of competency and education to achieve competency.

In this context, end user education can be valuable, but at the moment suffers from a number of problems, including a lack of a link between education and skills competency requirements and the general ineffectiveness and inefficiency of much cyber risk education.

In thinking about trying to influence end user behavior via education, ROAR has come to the view that the "driver license" analogy is appropriate, compared with say a swimming lessons analogy.

That is, ROAR is of the view that education will continue to be ineffective unless achievement of education outcomes is linked to the achievement of skills outcomes, which are in turn required before an end user is able to use the internet in various institutional contexts such as the school, the firm or a community organization.

In many contexts in society we do not allow people to undertake activity such as driving an automobile, operating heavy earthmoving equipment, handling chemicals etc, unless they can show they have the skills to do so safely without hurting others. In addition, the organizations in which they participate are required to have in place risk management programs to deal with the particular risks.

ROAR proposes that this approach be utilized in respect of management of cyber risk and the role of end user education in such management.

Specifically, ROAR proposes that a national Internet users license system be established.

Granting of such a license would require demonstration of defined skills competencies in avoiding and managing a range of cyber risks.

Education to achieve such competencies could be undertaken in a wide variety of contexts, such as the school, the firm, non-profit organizations, or the home.

Such education would use a unified national curriculum and largely involve on-line training and testing, in order to dramatically increase educational effectiveness and lower costs.

The costs would be subsidized to a limited degree by government, but also be born in part by the beneficiaries, namely: the end user (e.g. though use of their time in achieving certification); the various organizations where the end user spends time, such as schools, firms and non-profit organizations; and the providers of the pipes which are enabling the problem in the first place, such as via the NBN roll out.

ROAR is of the view that once a national standard had been established, working with the various user groups, compliance would spread rapidly, via schools, firms and community groups requiring their members to show they have the skills to manage cyber risk, as demonstrated via having been granted their license, before they are granted network access rights in an organization.

It is the experience of ROAR that the per capita costs of such a licensing, testing and training system are quite modest, compared with the costs of the risks averted.

2. INTRODUCTION

The purpose of this submission is for ROAR Film Pty. Ltd. (ROAR) to provide some observations regarding the subject of community wide cyber risk education, based upon it's experience in producing and delivering education packages in the K-12 education industry in this subject domain.

3. ROAR FILM PTY LTD – A SPECIALIST IN ON-LINE CYBER RISK EDUCATION

ROAR Film Pty. Ltd. Is a Hobart Tasmania based online education services provider specializing in cyber risk education.

ROAR has since the year 2000 been producing film and TV documentaries for a range of government and private organizations in Australia. In addition, in the last five or so years it has gravitated to the development of multi-media education resources for various clients in Australia, including the (national) Learning Federation. Along the way it's products have won numerous awards for quality.

Around three years ago ROAR was contacted by the London Grid for Learning (LGL), a broadband network linking all London public schools, regarding the production of an education program that would aid in the teaching of citizenship values. This lead to an ongoing relationship with the LGL and the creation of education products across the entire

cyber risk subject domain – through cyber citizenship, cyber risk and cyber safety, covering all of the key stages in the English K-12 curriculum.

In Australia, ROAR was also recently contracted by the Department of Broadband Communications and Digital Economy (DBCDE) to produce the education resources on the BUDD:E web site for use in K-12 cyber security education.

Today in England ROAR has sold licenses to 41% of all English public schools and the resultant services, for example, are amongst the top few most trafficked web sites on the London Grid for Learning, which encompasses all public schools in London and is an education system roughly the same magnitude as that of Australia.

ROAR believes that its experience in England in the cyber risk education market in the K-12 school sector, is relevant to Australia for a number of reasons, viz:

- ROAR specializes in the cyber risk education area – we believe we have developed a considerable base of expertise
- England is ahead of Australia in implementing broadband networks in it's public schools (although not for much longer), and the social context, as measured by the types of incidents reported, is probably around two years in advance of Australia
- The issues in England are very similar to those emerging in Australia
- Cyber risk education in the K-12 sector in England has gone through a number of phases which are likely to be roughly paralleled in Australia
- Some types of cyber risk education work and some do not

4. THE SUBJECT DOMAIN – CYBER RISK MANAGEMENT

4.1 Overlap of cyber security, safety and citizenship risks

ROAR notes that the domain of Cyber risk management covers three related subject areas, viz:

- Cyber security – such as various forms of intent identity fraud
- Cyber safety – such as various forms of intent based social bullying
- Cyber citizenship – such as intellectual property management and on-line ethics

ROAR notes that whilst each of these domains is separate, there is a very significant area of overlap, both in the subject matter and in the approaches to management of these risks.

For instance, whilst the theft of intellectual property is clearly an aspect of cyber crime (and thus security), it is also related to concepts of cyber citizenship and ethics.

4.2 Overlap of education regarding cyber risks

Similarly, education of target groups, such as secondary school students, regarding cyber risk issues, must inevitably canvass issues such as ethics of the pirating of intellectual property (a cyber citizenship topic) whilst also talking about the practical aspects of management of intellectual property theft (a cyber security topic).

In particular, the experience of ROAR suggests that any approach to educating the community about these issues needs to embrace all three subject areas.

4.3 Resultant overlapping policy and administrative domains

In addition, ROAR notes that this overlap in subject matter also raises the issue of domains of responsibility.

In Australia, at the Commonwealth level, there is increasing co-ordination between the various agencies involved in cyber risk issues, whether they be education, communications, crime, children's or traditional security related portfolios. Inevitably more could be done, but at least the legitimate roles of various players is recognized and means of policy co-ordination are being put in place.

Such co-operation is not yet reflected at the state and local levels, for most part.

For instance, at the level of the Head Teacher of a school, in most states there is no standardized means by which cyber risk incidents in schools are detected, measured, logged and reported to a range of agencies. Nor is there means by which they are then investigated or assistance is rendered to a Head Teacher by the police, health or children's services authorities. Nor in some states is it clear where the responsibility of Head Teachers for cyber risk management ends, particularly where it involves incidents occurring outside of the local school intranet.

This is in contrast to the UK where, whilst not perfect and still evolving, Head Teachers are aware of the extent of their responsibility for cyber risk incidents, inside or outside the school and there is a procedure at the local authority level to mobilize the responsible organs of government to deal with the issues.

5. A LEAP IN THE LEVEL OF RISK TO BE FACED

Whilst one can overemphasize some of the more headline grabbing aspects of the field of e-risk management (such as cyber bullying), there is nevertheless a quantum leap in the challenge faced by the community underway, due to the confluence of a number of factors, most notably:

- **A major expansion of symmetrical bandwidth down to the household and small business level that will within years rival the processing bandwidth of the human eye and brain (said to be around 2Gbps)** – leading to more and more computer and human based interactions moving into “the cloud” and thus being vulnerable to cyber risks (e.g cyber bullying is an early example of such a phenomena in the bullying world, but there are many others that can be envisaged as real time virtual reality and image transmission become possible, including the more sensational sexually oriented ones mentioned in the popular media)
- **The increasing portability of this bandwidth to anytime anywhere, through the rise of 3G and 4G mobile networks** – with the resultant increase in lack of supervised access and potential points of risk for the vulnerable (e.g. K-12 children operating outside of home or the class room, in the school playground, the shopping mall and whilst travelling, become unsupervised participants and targets); and
- **The advent of interactive applications that change the meaning of community** – as internet traffic moves from being mainly one to many and asymmetrical in terms of bandwidth usage, to one to one and more bandwidth symmetrical and thus increasingly difficult to police (e.g. It is easier to deal with bank website fraud or

sales of pornographic materials, than a group of teenagers abusing each other via phone transmitted video)

Much of this is well known. For instance, in the experience of ROAR, in the K-12 education industry, the experience of the last three years reflects these trends, viz:

- Two to three years ago Head Teachers in England were grappling with issues such as: ensuring children set strong passwords; were not surfing smut web sites; were not hacking the school intranet; and were not short messaging each other over the school intranet during class; and
- Today, in addition, they are increasingly dealing with issues such as: teachers who engage in inappropriate and stupid cyber behavior; incidents involving groups of students moving to the mobile domain outside classrooms and the school; and coming to grips with their potential personal liability for such behaviors which are increasingly difficult to directly prevent or police

However, K-12 institutions are still grappling with the consequences of this shift. For instance, most K-12 school cyber risk management measures appear to be still oriented towards stopping school children accessing inappropriate external www sites from within the walled school intranet community. They do not deal with the impact of the rapid expansion of mobile device based Internet connectivity in the school ground and beyond within the school community. Many schools have yet to face up to the fact, particularly at the secondary level, that bandwidth use by students in the playground can exceed the bandwidth used on the school intranet, yet the former is largely unregulated.

The “dark side” of the resultant potential risks appears to have been well understood and are being addressed by the Commonwealth Government, via it taking control of network security measures and investing in a significant expansion of capability in that area.

It is the community risk management and education side of the issue that is currently not well addressed. Policy and programs and private behavior in Australia in the areas of community cyber-risk management and education are frankly, running behind the UK, a couple of countries in Europe and some USA states. For instance, contrast the efforts of mobile phone carriers in the UK (and increasingly Europe) versus Australia.

6. THE BASIC PUBLIC POLICY PROBLEM – CYBER RISKS INVOLVE EXTERNALITIES

ROAR is of the view that the management of cyber risk in a community requires the acceptance of the basic proposition that there are two forms of potential market failure at work, viz:

- The actions of one person cause others deliberate (e.g. a cyber crime or a cyber bullying victim)) or unintended (e.g. costs, which the first party cannot be made to bear) costs, which the party causing the problem cannot be made to bear
- Poor cyber risk management is likely to aggregate amongst certain groups in society, such as the young

One way of drawing out these issues is to use analogies with other areas of social risk management.

6.1 The learn to swim analogy - highly organized but mainly voluntary

The cost of the failure to learn to swim, for a child or adult at the extreme is drowning. This cost is mainly borne privately by the victim and their immediate family, although even in this example there can be some social costs borne out of the need to offer life guard services at the local pool or beach, to protect people against freak events. In addition, sometimes society decides it is a good thing to protect people against personal stupidity and ignorance.

Society intervenes to attempt to reduce the risks associated with swimming mainly via:

- **Prohibition and guidance** – such as fences around private pools and restrictions on access to swimming pools if one cannot swim, usually in school related situations
- **Supervision** – such as a requirement that adults accompany a child when swimming at a public pool, or the provision of lifeguard services
- **Small group education** – via extensive learn to swim classes
- **Controlling the quality of the education inputs** - Using standardized awards, testing and curriculum, and standardized instructor training
- **Measuring and certifying the outcome of education** - competency testing and licensing
- **Public education via mass media**

In the end, however, learn to swim training, even though highly organized, is for most part, voluntary, perhaps mainly because the externalities borne by the community are not all that significant. Most of the costs are borne by the individual who cannot swim and their family and swimming is not an activity that most people need to engage in nearly every day.

6.2 The driver training analogy – highly regulated and compulsory

If a young person illegally drives a car, crashes and hurts others or themselves, the costs are borne both by the injuring and injured parties. That is, there are significant external costs imposed upon others by the driver. Consequently, a system of compulsory insurance and driver licensing has developed that aims to reduce the risks in the first place and secondly, to ensure there is some redress for those who bear the costs of the behavior of others.

The compulsory driver training system includes elements such as:

- **Prohibition and guidance** – such as not being allowed out onto the road without a drivers license and a comprehensive set of rules regarding usage of the roads and interaction with other drivers
- **Small group education** – via extensive learn to drive classes consisting of mainly one on one classes
- **Compulsory supervised apprenticeship** – such as a requirement that adults accompany a learner driver for 120 hours in NSW
- **Controlling the quality of the education inputs** - using standardized curriculum, instructor training and instructor licensing
- **Measuring and certifying the outcome of education** – standardized competency testing and licensing
- **Public education via mass media** – regarding various risks associated with driving such as speeding or use of alcohol

Reflecting the:

- Human costs at stake, both for the driver who injures themselves and for those they injure
- Which in both cases are to a significant degree borne by the larger society – for instance increased lifetime publicly borne costs of care of those who are injured
- Together with the widespread requirement that most adults drive and the resultant reasonable probability of accidents
- Together with a strong link between lack of driver skills and higher accident rates

the system of driver education has become increasingly compulsory in nature.

It is very doubtful that society would ever wish to revert to a system of voluntary driver education based upon community exhortation campaigns.

6.3 Internet use – spillover costs somewhere between driving and swimming

In the case of public and private use of the Internet, we have a situation that is more akin to the driving a motor vehicle, than swimming. For instance:

- **Use of the internet, like driving a motor vehicle, is a mass activity** that is engaged in by a large proportion of the population, most days
- **Some risky on-line behaviors hurt only the person engaged in the behavior and do not involve a second party deliberately causing harm to a particular user** - such as the potential consequences of engaging in prolonged on-line gaming upon a young persons personal development, or distribution of pornography, except where it exploits particular groups in it's production
- **Some risky on-line behavior involves two parties, where one party deliberately harms another** - such as internet fraud, or some cyber bullying, which impose costs upon careless individuals, or their corresponding parties, such as their bank, but not upon third parties
- **Some risky on-line behaviors impose costs upon whole groups of people** - Other behaviors, such as illegal file copying and sharing, infecting local networks with malware and viruses, some forms of cyber bullying that involve a group of say young people and the creation of botnets, impose costs upon a wider group of users than those who engaged in the initial problem causing behavior

ROAR does not have any reasonable measure of the privately borne or external costs caused by cyber-risk behavior, but notes that:

- Estimates of the privately born costs of cyber crime appear to be in the range of A\$10-100 per person in the population per annum
- Estimates of the costs of software used to deter viruses and malware are in the range of A\$1-10 per person per person in the population per annum

It would appear reasonable to guess that the total cost of both private and externally borne risk to the economy each year would be of the order of A\$100 per person in the population.

In sum, unlike driving, internet “accidents” do not kill you, but they certainly are more pervasive throughout the population than say swimming accidents and involve substantial community wide external costs.

6.4 Is cyber risk an equity issue as well as involving externalities?

Most of the submissions to the Inquiry approach cyber risk (in the cyber crime context) as an efficiency issue. That is, they show concern for the economic losses to the economy arising from privately and socially borne costs arising from cyber crime.

There is less evidence that cyber risk is disproportionately borne by any particular group, once they are educated regarding the nature of the risks and how to manage them in every day life.

In this sense, it is clear that any equity issue should primarily be dealt with by education, particularly of the young and other smaller groups such as more elderly users, who are not cyber savvy.

7. CURRENT PUBLIC POLICY APPROACH IS LOPSIDED

The previous section argued that there were substantial external costs that arose as a result of cyber risk and that to some extent these costs were distributed more towards naïve users.

Prima facie, there would appear to be a case for Government involvement in prevention and amelioration of risk, provided the costs were modest. It is worthwhile examining current approaches to this task.

7.1 Measures are weighted towards prohibition, investigation and exhortation

The activities associated with attempting to avoid or ameliorate these risks currently include:

- **Prohibition** - such as the contemplated national filtering system
- **Contractual** – such as requiring school children and employees to sign acceptable use policies where the user agrees to not engage in particular activity
- **Supervision** – such as not allowing children to use the internet unless under the supervision of a teacher or parent
- **Accident reporting, investigation and amelioration** – such as the activities of AUSCERT and the AFP working with the victims of cyber crime
- **Mass education** – such as the current activities of the federal government via ACMA and DCBDE, or via the web sites of various telcos and ISPs
- **Small group and personal education** – such as the teacher education and community briefing activities currently undertaken on a small scale by ACMA

ROAR does not belittle or pretend to have an expert assessment of the relative and complimentary effectiveness of many of these measures, but notes that what is striking is the relative lack of emphasis upon education of the individual Internet user and the associated infrastructure to deliver such education.

This situation is in striking contrast to many other areas of human behavior where there are externalities potentially generated by the individual behavior of Australians. Such areas include:

- The regulation of vehicle movements on public roads, where driver skills certification is mandatory

- The operation of various types of equipment in the workplace, such as heavy vehicles, or plant
- The regulation of occupational health and safety within the workplace
- The offering of various forms of advice or undertaking certain tasks, such as provision of financial advice or becoming a carer of a person with Alzheimer's disease

In all of these areas of human endeavor there is usually a policy framework in place that has the following elements, viz:

- To undertake a task safely the user is required to be certified to have certain skills
- Such skills are tested following the undertaking of some form of course
- The course has an agreed national curricula within the Australian vocational training system
- The people and organizations offering such a course also need to be certified as being competent

It is striking that none of this exists in the case of end user cyber risk education.

7.2 The relative importance of education versus regulation

Some forms of cyber risk cannot be dealt with by educating the user. This includes many of the more sophisticated forms of internet security violations, such as the creation of botnets. These forms of risk can only be dealt with by tackling the source of the problem and/or engaging in blocking type behaviors.

In addition, some acts of outright prohibition or practice, such as internet filtering in schools, can be useful for some target groups, particularly very young children, but in many cases these become ineffective as the individual user becomes more sophisticated.

Similarly, acceptable use policies, including those that are contractually binding, are useful in individual organizations as a means of limiting harm to the individual, the organization and others

However, many of the submissions to the Committee, from persons well qualified to make the observations, have spoken of the difficulty of staying ahead of the evolution of cyber risks. Some have spoken of the need to always complement regulatory or blocking behavior with preventative action, most notably user education.

ROAR supports this view across the entire spectrum of cyber risk management, including cyber security, safety and citizenship, with the caveat that in some areas of cyber security, education is of little value.

By way of example, the principals of ROAR have been involved with implementation of large scale internet deployments in schools in Australia and the UK for the last 10 years. It is our observation that whilst "walled garden" solutions to cyber risk issues are useful, they have major weaknesses, which render them at best to be a partial solution to cyber risk management issues in the school context. For instance, they:

- Have always suffered the problem of restricting access of users (whether teachers or students) from using resources outside of the walled garden which are legitimate education resources

- Can usually be easily defeated by the more advanced students in the student user community in short order
- Protect only school intranet based devices (which are heavily regulated) but which are increasingly not the most widely used devices by students, particularly as internet bandwidth moves out of the walled garden intranet and the sole PC at home, onto mobile devices (based upon public carrier 3G or 4G clouds), which are essentially unregulated other than at the public ISP cum carrier level and which are what the student uses in the playground, at home and in the shopping mall
- Can do little to stop risky peer to peer behavior, such as transmittal of botnet malware via USB memory sticks or blue tooth, or cyber bullying behavior, even within the walled intranet
- Do not deal with the problem of the community context of the school. In an increasing number of education and community jurisdictions, the community expectation and in some cases legal requirement, is that Head Teachers of schools must take responsibility for behavior arising from cyber risks, even if the behavior did not take place on the school intranet, did not involve a school supplied device, and in some cases took place out of school hours at home or in the local shopping mall

7.3 Skills certification should be an important element of any policy approach

Putting aside the impracticality of a solely regulatory based approach, there is also the issue of who should be responsible for “safe driving” on the Internet. As with driving a vehicle on the roads, ROAR is definitely of the view that regulation and education can be made to complement each other.

The corner stone principles should be:

- There should be clear “road rules” (acceptable use policies) for the Internet, particularly where the user is located within an institutional setting
- The “driver” (internet user) should be required to contractually agree to adhere to these policies in environments where there are potential significant externalities arising from non-compliance
- The “driver” (internet user) should be required to have obtained their “drivers license” (Gigabit User License) before they are allowed to use high risk “driving” environments
- Education and testing against national standards in order to obtain the users license should be readily available at low cost to the end user
- If the “driver” breaks the rules, then they should be sanctioned

8. DOES CYBER RISK EDUCATION WORK?

To advocate the use of education to compliment regulation is only useful if it yields useful changes in behavior.

8.1 Much current cyber risk education does not work

Over the last few years ROAR has engaged in consumer testing it’s products before releasing them onto the market and then following their use in schools. This has provided invaluable data as to what works and does not work in educational terms, when the user is motivated.

So, for instance, ROAR has learnt from this process that learning programs that are purely resource based are generally ineffective. In contrast, interactive courses that have an inbuilt test component are far more effective.

In the opinion of ROAR, most current cyber risk education does not work for one or more of four reasons, viz:

- The form of cyber risk is difficult to detect by the user
- The user has little incentive to engage in “safe” behavior – even if they are educated
- The user has little incentive to be educated
- The education itself is ineffective

Expanding upon each of these.

8.2 Education is ineffective when cyber risk is difficult to detect by the user

As previously noted, a number of forms of cyber risk are hard to detect at the end user level. These include situations where say a computer has become a zombie in a botnet, or some form of keystroke logging and reporting software has been installed.

Consequently end user education in such situations is at best likely to have a marginal impact upon the level of cyber risk. Nevertheless, it may still be useful in alerting the user as to why action should be taken and what action to take, once the risk has been isolated, such as rebuilding a machine if it has become a zombie.

There are, of course, many other types of cyber risk that are readily detectable, by the user and where education can potential make an impact. Such areas of risk include theft of intellectual property, identity theft, cyber bullying etc., all of which represent a fairly significant proportion of the perceived risks.

8.3 Education can be ineffective where the user has little incentive to engage in “safe” behavior, even if educated

Many cyber risks, however, do not originate in far off lands. They originate in Australia, wherever people are at work or play. They often also arise in situations where the actors are very well educated as to what they are doing, but have little incentive to engage in safer behavior. To give some K-12 examples, often in secondary schools there will be a small community of “go to” students who are experts at defeating school on-line security systems. Similarly, those engaged in cyber bullying often know precisely what they are doing. Finally, a significant proportion of students engage in on-line intellectual property theft, knowing full well what they are doing.

In these cases education is useful in ensuring that the person understands the risk, but ultimately, there needs to be a series of clearly laid out rules and sanctions, which can be invoked. So for instance, in a K-12 school, or a firm, the acceptable use policy and associated sanctions need to be clearly laid out and enforced.

8.4 The user has little incentive to be educated

Even if the rules and sanctions are well understood by individuals in an institutional setting such as a school, firm or non-profit organization, there can still arise the problem that the individual puts off becoming educated, even if they have signed up for various codes of

behavior. For instance, in the K-12 setting, many students and teachers often overestimate their skills in managing cyber risks.

It is the experience of ROAR that the only way of ensuring people have the required skills to deal with many cyber risks, is to require them to be certified as possessing the skills, based upon competency testing and to tie network access to possession of such certification.

For instance, in a K-12 setting, requiring students to possess a certain level of demonstrated skills before they sign up to an acceptable use policy and gain graduated network access rights, provides both a good set of incentives for students and teachers to acquire the skills, but also removes any excuse at a later date that they did not know what they were doing, when they engaged in risky behavior.

8.5 The education is ineffective or inefficient

Even in situations where it is agreed that if the user possessed some skills risks might be reduced, the education to acquire these skills might still be ineffective. For instance, it is clear that the end user can largely control on-line identity theft, but the education to reduce this risk can often be ineffective.

In the opinion of ROAR much of what passes for cyber risk education falls within the category of being ineffective. That is it just does not work. It does not lead to the citizenry having a set of competencies, which would allow it to protect itself against many cyber risks.

In the K-12 setting, typical program effectiveness mistakes made in such education include (there are many others!):

- Some so called education campaigns are awareness raising activities, of limited use to anyone, apart from promoting panic
- Many education programs consist of “throw it over the fence” style resources (typically web sites with lots of links and lengthy pieces of text which to students are boring), which assume that either the end user directly, or via a teacher, can use these resources to effectively learn
- Assuming that teachers can take generalist resource materials and use them to construct appropriate class room activities, an assumption that is often wrong given the lack of time, professional skills (and thus training) of the teacher in this subject area
- Resources and activities assume there is such a thing as a typical student, when there is not – for instance a Year 9 student in terms of cyber risk management skills competency, can in reality have a “cyber age” of at least 8 years around a mean. Consequently, activities pitched at the mean are ineffective for a large proportion of students

Again in the K-12 setting typical program efficiency mistakes, include:

- Relying upon expensive, inflexible, face to face seminars as the means of educating the teaching workforce regarding cyber risk issues. At the current rate of training, Commonwealth sponsored teaching training regarding cyber risk will take many years to visit each K-12 teacher once at a high unit cost
- Similarly, relying upon teachers in K-12 classrooms to formulate lesson plans using externally provided resources is an inherently inefficient way of educating young people about cyber risks

8.6. Characteristics of cyber risk education that works

From the experience of ROAR in the K-12 sector, the characteristics of approaches to education that work are:

- The school or firm has in place an enterprise wide cyber risk management program that can link risk, to use of networks, to certification of competency
- Certification of the skill outcomes of education is rewarded within the school or firm
- The education or training is skills competency based – that is the student does not have to repeat materials if they can pass the test and they move on to a higher level of training which is then rewarded
- The education itself is not dependent upon the skills of trainers or teachers to deliver it – that is it uses largely on-line delivery, with trainers or teachers becoming mentors or tutors
- The education uses highly interactive objects that not only teach the relevant skills but also has inbuilt testing and uses competition between students to promote learning
- The nature of the learning objects changes according to the skill competencies and social maturity of the students
- There is a reporting system that appraises relevant parties, such as teachers, Head Teachers, parents, as well as students, of the progress of an individual student and a class
- It is inexpensive compared with the costs of the risks averted

9. THE SCALE OF THE LEARNING TASK – SUBSTANTIAL, EVOLVING AND INCREMENTAL

A question that arises when considering cyber risk education is the extent to which the skills that need to be taught are a significant body of knowledge or are of a relatively trivial nature, and to what extent is the body of skills rapidly evolving? The answer to these questions impacts where and how any such education needs to be imparted.

It is the experience of ROAR that the subject domain or required curricula, has the following characteristics.

9.1 The body of knowledge is substantial

ROAR, working with the English school authorities, has evolved a full K-12 curriculum, which covers cyber security, cyber safety and cyber citizenship. The body of knowledge continues to grow as time goes on. The order of magnitude of the knowledge embodied within this curricula is somewhere between that of a module in a university course and a full university subject (e.g. 30-140 hours of learning required). The nature of the skills, however, is that many of them are best taught through “learning by doing”

9.2 The skills required of users are roughly similar across the internet user population.

With some tweaks to allow for age related differences and industry of the user, the skills required are similar for all users. For instance:

- Learning objects that aim to teach the formation of strong passwords for adults, will be different in learning process and presentation, than those directed at 6 year olds, but cover essentially the same topic.

- Whilst everyone, no matter where they are a user, such as at home, at school, or at work, has a need say to learn about phishing, other elements of curricula such as cyber bullying issues should probably be directed mainly at adolescents

9.3 The skills required are evolving due to new technology

As the nature of the subject domain changes there are new skills required. For instance, two years ago there were few high bandwidth 3G mobile devices deployed in secondary school playgrounds and social networking was just starting to penetrate the school age population. Today they are becoming more ubiquitous and as a result the course content needs to evolve to deal with the additional issues that arise from these new technologies

9.4 Generally the new skills are additive, to the sum of required skills

As the Internet has evolved most of the skills required in the cyber risk management area have either stayed similar or needed to be upgraded. For instance the need for strong passwords was present 10 years ago and remains a valid issue today. New issues such as managing schoolyard cyber bullying add to this base of knowledge.

In total the body of knowledge which has emerged over time suggests that a competent adolescent or adult user of the internet needs to have a set of skill competencies which are roughly equivalent to the Cert 1 level within the Australian Qualifications framework and that there is a need to periodically refresh and bring up to date these skill competencies.

10. WHAT IS THE CORRECT POLICY FRAMEWORK FOR CYBER RISK EDUCATION?

10.1 Some limitations of current cyber education programs

The Commonwealth Government, as part of it's announcements regarding internet safety and security has invested in public education campaigns regarding cyber security and cyber safety. It has also committed resources to the Alannah and Madeline Foundation to undertake a pilot of a school based cyber safety accreditation program.

Whilst a positive start, these initiatives would appear to have some weaknesses, which will need to be addressed.

- **Governments are not providing a clear message to citizens regarding their mutual obligations and commitments** - On the one hand the need for all citizens and organizations to become skilled internet users, well able to personally guard against the risks; and on the other hand the responsibility of governments to set national skills competency standards; to seed the market for provision of educational services; and to provide for the more vulnerable. To also set out the obligation for citizens and organizations to report e-risk incidents, but also for governments to have incident management systems and resolution services in place.
- **An emphasis to this point upon "throw it over the fence" type programs** - Which result in numerous government funded "resource" web sites and pilot programs for various groups, whether they be students, teachers, or parents, none of which appear to have enough resourcing, none of which are effective on a mass market basis and all of which discourage the development of proper outcomes oriented markets. For instance, at the current rate of implementation, it will take many years

for current state and federal programs to provide a basic education about cyber risk issues for teachers in the K-12 system.

- **A lack of mobilization of market forces to rapidly achieve results** - A tendency in Commonwealth programs to implement approaches which require Commonwealth public servants to do most of the delivery or hire consultants to assist, rather than the UK and EC approach which is to create proper regulated standards governed markets to solve the problem and to subsidize these markets only where there is a clear case for subsidy.
- **A lack of use of Commonwealth resources to mobilize private resources** – the cost (based upon ROAR experience in the UK) of modern on-line testing, training and re-testing in this field is around A\$12 per family per year. The costs of ongoing CPE for teachers and trainers to keep them up to date is around A\$150 per year. Mobilizing such amounts from within existing household and institutional budgets is not a major issue. Government subsidies need to be put into kick starting such markets, and setting out the regulatory framework, which should then become self-sustaining.
- **A lack of focus upon the workplace, community organization or school level as the point at which policy needs to bite.** An exception here might be the pilot study commissioned from the Alannah and Madeline foundation regarding cyber safety
- **A weakness in administrative arrangements** at the Commonwealth and state levels and between levels of government. Undoubtedly, at all levels of government and within the broader community there are multiple legitimate interests including: national security; criminal activity; child protection; education; and network supply and regulation. Nevertheless, there would appear to be weaknesses in the arrangements, particularly at the local level between the education system and other agencies.

10.2 School, community group and workplace risk management the main focus

A couple of the above mentioned points require expansion.

Inevitably the question arises as to where to best reach the various target groups to educate them regarding cyber risk management, assuming that it is accepted that education is a desirable thing.

Cyber risks can be seen to arise in various settings:

- **All risks involve individual users** – So it might be argued that education and management efforts should directly target the user. For instance all users should be required to obtain skills certification before using any internet service
- **The end user utilizes a set of pipes or carriers** – So perhaps ISPs or mobile telcos should assume responsibility for cyber risk education of end users. For instance, before a user can be signed up to use the NBN, they must be educated
- **The user is usually at home, school or at work when the risks are present** and much of the resultant spillover (externalities) impact of risk taking is borne within the confines of these institutions – So we should aim to have these institutions take responsibility for cyber risk education

It is ROAR's view that education campaigns that attempt to solely target the individual user, or solely target the users of a particular pipe to the customer (such as the carriers or ISPs), will not have high success rates with the general population, due to the lack of the incentive for the user to conform to the expected behavior and the lack of a social context for the user.

To expand upon this point, whilst some users can operate independently of social groups and learn the appropriate skills on-line, this group is likely to be a small group of persons who are already technically inclined.

Combining on-line learning with a social or peer group context, such as through a school, firm or community organization, together with a reward, such as a certificate and/or access to network resources, dramatically increases the chances that the great majority of persons will be willing to engage in the education.

For instance running a competition between students at a school to see who can achieve their Internet drivers license first, is more likely to yield a result than parents trying to force their children to do a course at home.

For instance, having a group of senior citizens undertake a cyber risk course as a part of their internet skills course in their local senior citizens club, is likely to be more effective than having the same folks sit purely at home doing the program.

It is therefore the view of ROAR that the education effort should primarily be made via social settings in which most people are engaged, such as within the company, the school or community organization and should involve a standard framework that works in any of these contexts.

However, this does not necessarily mean the providers of the pipes have no responsibility for education. They may not be the best point of intervention for the provision of education, but they have an interest in reducing risky behavior and it is the expansion in the capacity of their pipes that is enabling a potential quantum leap in the level of risk.

It would seem reasonable that in the context of the NBN implementation, the pipes providers might need to make a contribution to dealing with cyber risk education issues.

10.3 Potential means of encouraging compliance

At the heart of the argument in this submission is that there is a mixture of private and external, or social, benefits resulting from an increase in the skills of the citizenry to use the Internet safely.

Accordingly, it is also clear that the costs of any such up skilling should be split in some appropriate manner between public and private players. So, for instance, the costs of dealing with electronic bank fraud are mainly borne by the bank and it's customer and probably should be borne by them, whereas the costs of cyber bullying involve some broader externalities, which should involve the community sharing part of the costs of preventative education.

With these principles in mind, it is appropriate to examine the possible points at which private compliance might be encouraged, with at least some of the costs being borne privately.

The “points of compliance” in general are likely to be in contexts where an institution bears significant external costs if the user fails to implement risk reduction procedures in their use of the Internet at that institution. This principle would appear to apply in a wide range of settings, including students at schools, workers in firms and community members volunteering in community groups.

For instance:

- A student wishing to use the intranet or a personal mobile device at a school having to show they have the appropriate level of certification to reach a particular use level. This can be enforced via signed contractual like acceptable use agreements.
- The benefit for the school might be as part of its compliance with a recognized Australian standard, which if their school were private, would lead to a professional indemnity insurance discount
- At the point at which a consumer joins a large expansion in their bandwidth, such as the NBN, which exposes them to greater risk
- Being in a profession that interacts with children or customers, where the internet is used
- Belonging to a community group that interacts with children on-line

10.4 Setting national standards

In numerous other fields where there are risk issues involving, firm level externalities and both personal and institutional responsibility, behavior and skills competency, national frameworks have emerged to manage risk that often have the following components, viz:

- Application of a standardized risk management framework (e.g based upon AS4630) to assess risk at the organization level (whether it be a school, community organization or firm)
- The result is usually a plan that sets out the risks, puts in place plans and actions to try and reduce or avoid them and sets out how incidents are to be reported, recorded and handled
- Individuals within the organization who wish to engage in particular activities, are required to have a certificate of skills competency against a national skill standard
- Standardized national programs of skills training are then used to train the members, students or workforce of an organization
- Persons who wish to deliver these packages are themselves required to be certified as competent trainers, against a national standard

This approach is widely used within the Australian vocational training system to deal with skills training regarding risks ranging from the risks associated with running a mine, to training carers of persons with Alzheimer’s disease, through to dealing with chemical hazards.

Outside of some quite specialized aspects of network management, this approach has not been used in dealing with cyber risk.

ROAR has begun to implement it in England as a result of requests from its UK customers.

11. PROPOSAL – A NATIONAL GIGABIT USER LICENCE

In the view of ROAR, successful cyber risk mitigation amongst the general community will require an approach to community cyber risk education that might include (in addition to regulatory programs):

- **A commitment to the achievement and maintenance of national competency standards in cyber-risk management by all Australian citizens and their organizations** – on a voluntary basis amongst groups such as parents, or older citizens and on a compulsory basis where a citizen uses school, firm or organizational infrastructure where their behavior has a potential external effect upon other citizens or organizations
- **For organizations this would involve a commitment to implementing standards based risk management plans** (e.g based around AS4630 - soon to become ISO31000) in the management of cyber risks. Again largely due to the externalities that lack of compliance by some causes for others, this will need to be compulsory in some sectors, such as in secondary schools, where there a very real community spill over effects
- **Testing against and education to meet, national skills competency standards** – this can be packaged via the existing national skills training arrangements – for example, most Independent school peak organizations at the state level are already registered training organizations delivering teacher professional development courses
- **Establishment of a nationally branded cyber-risk incident reporting and advice service**, in co-operation with the states and relevant community organizations
- **Commonwealth encouragement** for implementation of the framework could be via measures such as:
 1. Putting this in place, associated with the NBN investment – if a state or region wants the NBN investment then they need to put in place the e-risk management framework
 2. Encouragement of insurers to adjustment insurance policies to favor compliant organizations such as schools or firms
 3. Adding conditions to the DER grants that schools receiving support need to meet national institutional risk management standards (AS4630 related) and national teacher and student skills competency standards
 4. Speedy recognition for credit of the student, worker, parental and teacher skills competencies within the AQF
 5. Encouragement and regulation if necessary, for all carriers to educate their customers
- **Provision of government subsidies directly to schools and other organizations** to encourage them to initially implement the organizational standards.
- **Provision of government subsidies to parents, students, workers and teachers** in specific circumstances to initially encourage them to undertake the testing and training

- **Use of exemplar community and sector specific pilot implementations**, such as via the NBN roll out in Tasmania, as environments where such a framework might be implemented