

**21 Castle Hill Drive South
Gaven.
Queensland. 4211.
Australia.**

**Phone: 07 – 3138 9451 (Office)
07 – 5502 2978 (Home)
Email: w.caelli@qut.edu.au**

The Secretary,
Department of Broadband, Communications and the Digital Economy (DBCDE)
Canberra. ACT.

Email: DEFutureDirections@dbcde.gov.au

4 February 2009.

Dear Secretary,

I am pleased to be able to attach my submission to your "*Digital Economy Future Directions Consultation Paper*". This submission is made on the basis of over 45 years experience in the ICT industry in Australia and overseas as well as specific experience in the information security / assurance area for over 35 years.

I would be pleased to answer any questions or to clarify any specific point as you deem appropriate. The above address is that of my residence.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'W J Caelli', written in a cursive style.

Professor Emeritus William J Caelli, AO

**SUBMISSION TO:
Digital Economy Future Directions
Consultation Paper.**

Professor Emeritus William J (Bill) Caelli, AO
Senior Research Scientist
Information Security Institute (Level 7, 126 Margaret Street)
Queensland University of Technology
GPO Box 2434
Brisbane. Qld. 4001

Contact:

Phone: 07 – 3138 9451

Email: w.caelli@qut.edu.au

The content of and opinions expressed in this submission are those of the author and not necessarily those of the Information Security Institute or the Queensland University of Technology.

1. PROCESSES IN THE DEVELOPMENT OF THIS SUBMISSION.

DIRECTION AND LEADERSHIP FROM AUSTRALIA'S PRIME MINISTER.



Good policy is one thing.

*But good policy without **effective program implementation** is a dead letter.*

Evidence-based policy

*A third element of the Government's agenda for the public service is to ensure a robust, **evidence-based policy making process.***

Policy design and policy evaluation should be driven by analysis of all the available options, and not by ideology. When preparing policy advice for the Government, I expect departments to review relevant developments among State and Territory governments and comparable nations overseas. The Government will not adopt overseas models uncritically.

We're interested in facts, not fads.

The Prime Minister – The Hon Kevin Rudd
Address to Heads of Agencies and Members of Senior Executive Service,
Great Hall, Parliament House, Canberra
30 April 2008

The above two principles clearly emphasized by Australia's Prime Minister in a 2008 speech, namely the need for *effective implementation* and *evidence based policy formation*, have influenced and directed the work involved in the preparation of this

submission. In particular, the reported sentiments of Australia's Prime Minister from a national newspaper, the Weekend Australian of 31 January 2009, have also been carefully considered in the formation of this submission. These sentiments were reported as follows:

*The Prime Minister has vowed to use the "greatest market failure" in 75 years to commit his Government to **sensible new market regulation and intervention** to stabilise the economy and save jobs.*

Mr Rudd says the "ideology of the unrestrained free market, discredited by the Great Depression", re-emerged in the 1970s and was promoted by the Reagan and Thatcher governments in the US and Britain and became the "economic orthodoxy".

Source: The Weekend Australian 31 January 2009.

These words were in reference to an essay of the Prime Minister, published in February 2009 that clearly sets out the bases mentioned above and those which have naturally and rightfully influenced this submission. Those words of Mr Rudd are:

From time to time in human history there occur events of a truly seismic significance, events that mark a turning point between one epoch and the next, when one orthodoxy is overthrown and another takes its place.....

There is a sense that we are now living through just such a time: barely a decade into the new millennium, barely 20 years since the end of the Cold War and barely 30 years since the triumph of neo-liberalism - that particular brand of free-market fundamentalism, extreme capitalism and excessive greed which became the economic orthodoxy of our time.

Note:

This was exactly the period of the explosive development of the ICT industry, including the actual creation of a new "software industry", with its entry into the commodity product marketplace, essentially dominated by USA based enterprises. Thus an emphasis on essential market intervention is a central theme to this submission as another seismic change occurs, movement to a "digital economy".)

2. SUBMISSION.

ANSWERS TO AND OBSERVATIONS ON SPECIFIC QUESTIONS:

A. General Topics:

What categories of Public Sector Information (PSI) are most useful to industry and other stakeholders to enable innovation and promote the digital economy?

Noted – No comments

What are priority issues that will facilitate the use of PSI?

1. Text Only Web Services:

If, as seems likely, next generation broadband services will not be available at reasonable price to regional and city fringe people and enterprises alike for a period of up to three years or more from the present, all Federal Government websites, where PSI systems are created and maintained using so-called “web services” technologies or similar, will be offered in “text only” form in addition to any active, graphic form. This will be MANDATORY specification in all PSI systems to be developed or are currently under development and shall be incorporated into currently existing systems where this facility is not present as a matter of urgency.

Where graphic systems, video/audio streaming or allied systems are placed into the server website, such systems shall be guaranteed NOT to take primary control of the data link to the end-user under any form of priority.

(Special Note – Evidence:

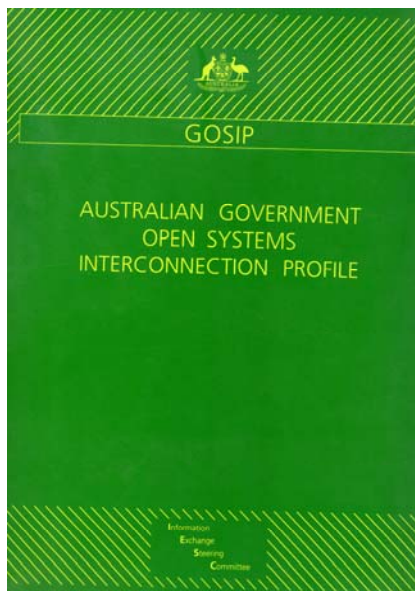
At low, dial-up speeds and even at medium speeds below 1Mbit/sec such subsystems effectively perform a “denial-of-service (DOS)” operation on the end-user system.)

If PSI is made open access, what are the best formats to enable and promote use and reuse?

2. All Interfaces will be Open.

The Australian Government, along with many other governments around the world, propagated the concept of “Open Systems Interconnection (OSI)” from the mid 1980s to the mid 1990s. Indeed, the Australian Government put forward its own

“Government Open Systems Interconnection Profile (GOSIP)” but then, from all evidence available, largely ignored it! Indeed, for example, Microsoft Inc.’s “Windows’NT” operating system in the early 1990s was apparently developed with the USA Federal Government GOSIP designated and IEEE standardised “POSIX” application programming interface standard included to meet mandatory USA GOSIP requirements. This is an important example of Government purchasing being used to implement appropriate public policy settings.



Principle (The Principles of Australia’s GOSIP):

Proposal:

The Australian Government will mandate and ensure that all suppliers of ICT products, systems and services deployed in any government information system, or in any information system offered by any of its agencies or supported organisations, will make ALL:

- programming interfaces,
 - file, data and message formats,
 - data communications protocols and formats at all levels of the industry accepted 7-layer OSI model,
 - “middle-ware” and allied generic application system formats, and
- any and all systems specifications and any other necessary and relevant specifications OPEN and AVAILABLE for any Australian or other entity to create and interface any ICT products, hardware or software based, to those Government systems and for the user of any such public sector system to also readily interface to those systems. It will also be required that such specifications will be made available at reasonable cost.

It should be noted that the Australian Government did at one time, even sponsor an OSI compliance centre to check that agreed and open interfaces existed in all systems to be procured by the Australian Government and to aid industry in GOSIP compliance in general.

3. No Proprietary Enforced Interface requirements.

For example, it will be an illicit and illegal act for a Federal Government Department, for a start, to require an Australian citizen, SME or any enterprise to use a proprietary computer or data communications product, system or service in order to make use of any PSI. Where this may exist at present, such Federal Government Department shall have a period of one year to correct the situation. This principle will be recommended by the Minister to Australia’s State and Local Governments.



(Note: Mandating a proprietary system is equivalent to telling an Australian citizen that they can only visit their Parliament House if they drive there in one brand of car!)

Example:

It will be made illegal for a Government Department to only offer PSI interconnection for users of Microsoft Inc of the USA's operating systems, middleware products, application packages or Internet browser systems or to develop or contract the development of information systems that "lock" those systems into the products of that company in such a way as to require the end-user to use products of that company alone..

A minimum requirement, for example, will be access to PSI from other workstation or like computer systems using Microsoft's "Windows" OS products, Apple MAC systems, SUN Solaris and LINUX/ BSD (UNIX derivatives) based PCs and server systems, as appropriate, and from browsers such as FireFox, Opera, Internet Explorer, etc.

(Evidence:

The Australian Taxation Office and the "Microsoft ONLY" interface as reported in the press in December 2008. Copy attached at end of this submission.)

If PSI is made open access, what licensing terms would best facilitate and promote its use and reuse?

No comment provided.

Should licensing terms distinguish between commercial uses and non-commercial uses and reuses?

Noted

Are there other examples of innovative, online uses of PSI?

Noted.

Is there any additional economic modelling or other evidence to show the benefit to Australia from open access of PSI?

Noted

What more can industry and other stakeholders do to address concerns about consumer privacy and online safety?

Solution 1:

Development and enactment of balanced legislative action to govern security of products, systems and services offered by the ICT industry itself and the owner/operators of information systems used by individuals and enterprises alike.

The “*laissez-faire*”, “*light touch*”, “*market forces*” attitude of Governments worldwide in relation to the ICT industry has been commented on for over the last 30 years and, lately, by the Prime Minister of Australia in more general terms. Interestingly, the rapid changes in the ICT product and systems industry, heralded by the development and supply of “commodity” level products coupled with the creation of a new “software industry”, occurred during the same period as the now apparently discredited policies mentioned by Australia’s Prime Minister above.

Whereas Governments have been quite active in creating appropriate legislative and regulatory environments for other industries and service providers, e.g. the motor vehicle industryⁱ, pharmaceutical product manufacture and distribution, air transport, etc. little to nothing has been done in relation to the computer industry, particularly as the world moves to a globally connected Internet. This attitude has meant that the industry has not addressed the needs for information assurance required in its products, systems and services.

It is time to stop blaming and placing full responsibility for information security on the customer and the end user. It is time to blame and regulate the supplier of ICT systems and the owners/operators of related services.

The result is the information insecurity situation that is current. The term “industry”, in an Australian context as distinct from elsewhere in the world, is taken here to encompass both the suppliers and importers of ICT products and systems as well as the owners and operators (users) of those systems to provide vital information services to their customers, clients and allied entities as part of the “digital economy”, e.g. the banking and finance industry, the healthcare sector, Federal, State and Local government, etc. Attention is directed to just one aspect of the problem, i.e. the loss of intellectual property held in information systems globally. A recent report, presented at the Davos 2009 meeting, saw losses in this area as exceeding **over 1**

ⁱ Motor Vehicle Standards Act 1989, Act No. 65 of 1989 as amended.

Objects of Act: The main objects of this Act are:

*(a) to achieve **uniform vehicle standards** to apply to new vehicles when they begin to be used in transport in Australia; and*

(b) to regulate the first supply to the market of used imported vehicles.

It is submitted that this type of Australian Government Act is exactly what is needed in relation to the products, systems and services of the ICT industry in Australia.

Trillion US dollars annually. The McAfee Inc report outline is attached to this submission.

In summary, the current acknowledged poor security situation in which a digital economy is forming has the following factors involved.

- Governments, regulators and industry alike have been totally absorbed in “blaming the end-user” for the lack of security in the use of commodity ICT products and system, and in end-use information systems in both the public and private sectors, through websites, brochures and the like advocating “safe and secure” practices when using the Internet and the commodity PC for vital commercial and allied transactions. Nothing at all appears to have been done to regulate the ICT industry itself. End users are asked to perform the largely impossible, i.e. to protect themselves, while using acknowledged insecure systems, from sophisticated attacks while being totally inexpert in the technology involved.
- There is no evidence that safety and security enhancements to products and systems have ever happened through market forces or voluntary manufacturer or operator willingness.
- There is **no evidence that industry self-regulation has succeeded** in the creation and offering of secure computer systems and allied data network products, systems or services.
- The add-on security industry for ICT systems should largely not exist and only does because of a failure in regulatory authority and action in relation to the ICT industry itself. This causes the acceptance of massive additional costs by user organisations and end-users alike as it is widely acknowledged that it is far more costly to add-on security into existing information systems rather than have that security designed in from the start.ⁱⁱ.

This has become absolutely clear in the so-called “*finance industry meltdown*” now being experienced globally and apparently originating from the USA. Indeed, in advanced technology arenas, legislative response seems largely to happen as a reaction to a problem rather than any attempt at forward planning.

ⁱⁱ *Schneier Questions Need for Security Industry*

By Will Sturgeon, CNET News.com , April 30, 2007

Outspoken author and security guru Bruce Schneier has questioned the very existence of the security industry, suggesting it merely indicates the willingness of other technology companies to ship insecure software and hardware. Speaking at Infosecurity Europe 2007, a leading trade show for the security industry, Schneier said, "the fact this show even exists is a problem. You should not have to come to this show ever."

"We shouldn't have to come and find a company to secure our e-mail. E-mail should already be secure. We shouldn't have to buy from somebody to secure our network or servers. Our networks and servers should already be secure."



Mr B Schneier is the Chief Security Technology Officer of British Telecom.

In relation to the IT industry the former USA “cyber-czar”, the former Presidential advisor Richard A Clarke gave, in a media interview in 2003 (USA’s PBS Frontline program, 18 March 2003), the warning given in the box opposite.

“If there's a major devastating cyberspace security attack, the Congress will slam regulation on the industry faster than anything you can imagine. So, it's in the industry's best interest to get the job done right before something happens.”³⁵

He continued later in 2007 with the following statement:

According to Richard Clarke, former U.S. counterterrorism czar, who shared the opening keynote address slot with Sager, the government's culture must change a lot more before the country's critical infrastructure can be secured.

'I'd like to know why it was that we lost momentum in solving the problem in more than a piecemeal manner,' Clarke said in an interview with Government Computer News. 'There is no leadership. There is no national plan implemented.'

Industry, commerce, health care and national defense increasingly rely on an Internet that remains brittle and open to attack and disruption, Clarke said. 'The day-to-day environment is replete with crime and espionage. We are accepting a high level of cost we needn't accept. But we've done nothing to solve the problem.'

Government Computer News, 10 August 2007.



The problem is that the majority of public sector websites and allied brochures, advice documents and the like only address the end user of computer and allied data network systems and not specific requirements on manufacturers, suppliers and owner/operators of information systems. This is totally unbalanced and must be recognised as such and remedied as a matter of urgency.

Legislative Action:

a. Australian Government Leadership.

A balanced approach, as advocated by Australia’s Prime Minister, Mr Rudd, does mean that there is public sector and government action needed in line with the philosophies of a “mixed economy”, long espoused in Australia in the post war period by all political parties. The Australian Government must develop and enact instruments that address the same intent as that shown in the USA’s “*Federal Information Security Management Act (FISMA)*” of 2002. Such an Act will enable importers of information technology products and systems, as well as local developers, owners and operators of use level information systems, in “vertical” application areas, to be able to influence manufacturers and suppliers.

b. Formal designation of the National Information Infrastructure as a Strategic National Asset for national security, defence and legal purposes.

In line with current discussions in the USA, the Australian Government should designate the national information infrastructure (NII) as a “strategic national asset”. The appropriate defence implications of this should be researched and discussed.

c. OECD / United Nations Cooperative Efforts on the ICT Product and Systems Industry.

Action:

The Minister for DBCDE will actively lobby internationally for balanced regulation of the ICT industry in pertinent forums including the OECD and the United Nations. In particular this will extend, in cooperation with the Prime Minister, into appropriate legislative and governing arrangements for those enterprises offering information systems as part of a national digital economy, e.g. the banking and finance industry, retail industry, healthcare sector and the like,

Case Study Evidence in ICT Industry Failure to Secure its Products
Microsoft Inc's NGSCB – A Case Study in the ICT Industry.

Newsweek, 1 July 2002

Newsweek
▶ Home Page ▶ Cover Story ▶ Archives ▶ Feedback ▶ Index
Technology & Science

(from top to bottom) Bryan Willman, John Manferdelli, Paul England, and Peter Biddle of Microsoft are helping to make PCs more secure

The Big Secret

An exclusive first look at Microsoft's ambitious-and risky-plan to remake the personal computer to ensure security, privacy and intellectual property rights. Will you buy it?

By Steven Levy
NEWSWEEK

Brian Smale for Newsweek

On [August 28 2003](#) Microsoft made an announcement saying that to combat the thread of future viruses like [SoBig.F](#) a new approach to overall computer security was needed. This approach which had been previously announced and described became known as the "Next Generation Computing Base (NGSCB), preliminary codenamed as the "Palladium" project.

July 1 issue — In ancient Troy stood the Palladium, a statue of the goddess Athena. Legend has it that the safety of the city depended on that icon's preservation. Later the term came to mean a more generic safeguard.

Simon Conant, a 'security expert' (quoted verbatim from the source article, the [UK Metro](#)) working for Microsoft said in simple terms that

"We need to go back to the drawing board with a brand new architecture for the PC".

(Source: http://knowledgerush.com/kr/encyclopedia/Palladium_operating_system/ at 31 Jan 2009.)

The above report went on to state as follows:

Availability

*When originally announced, NGSCB was expected to be part of the then next major version of the Windows Operating System, Windows Vista (then known as Longhorn). However, in May 2004, Microsoft was **reported to have shelved the NGSCB project**. This was quickly denied by Microsoft who*

released a press release stating that they were instead "revisiting" their plans. The majority of features of NGSCB are now not expected to be available until well after the release of Windows Vista. However, Vista includes "BitLocker", which can make use of a Trusted Platform Module chip to facilitate secure startup and full-drive encryption. TPMs are already integrated in many systems using Intel's Core 2 Duo processors or AMD's Athlon 64 processors using the AM2 socket.

The NGSCB, and its associated security hardware module, the "Trusted Platform Module (TPM)" essentially provides, BUT only with associated hardware modification to the main computer itself, the CPU, the equivalent of a trusted PINPad unit in a PC, mobile phone, PDA or the like. This fact was recognised by the USA's national newspaper, USAToday on 24 June 2002 with the following statement:

Under Palladium, Intel and AMD will redesign computer processors to include cryptography features. Palladium also will require changes to video and keyboard technologies to ensure that a customer's typed information is displayed without changes on the screen.

The TPM alone does NOT provide that facility but does offer some increased level of data security for the digital economy with such facilities as full hard disk encryption services, etc. the original "palladium" project, as exposed to the public in a July 1, 2002 issue of the USA's Newsweek magazine, had a clear and precise statement that indicated that, for security in the digital economy age, the PC had to be REMADE to "ensure security, privacy and intellectual property rights."

It did not happen for the general public and PC consumer.

The then statement by a Microsoft manager in that Newsweek article is worth repeating in relation to the development of the digital economy, as follows:

Even more important, Palladium is intended to become a new platform for a host of yet-unimagined services to enable privacy, commerce and entertainment in the coming decades. "This isn't just about solving problems, but expanding new realms of possibilities in the way people live and work with computers," says product manager Mario Juarez.

The important policy development factor here is that industry by itself has not redeveloped the PC or any of its derivatives today for enhanced security, such as the expanded mobile phone using similar operating systems and Internet browser software. These products offered by the ICT industry itself form the basic connectors to the Internet and thus to the development of the digital economy. For security in the digital economy, the move to "data security" is the vital transition from protecting "data on the move".

In other words, from a security point of view, and for trust in the digital economy,

IT'S NOT THE NET, IT'S THE NODES

that matter. The major consideration today in relation to trust and confidence in the digital economy and its structures has moved to the problem of "data security". The data collections are the valued assets to be protected and this factor points to the need to harden the basic computer and database systems involved. So-called "perimeter" security is no longer sufficient whereby total information system security is made to depend upon security technology and products inserted into the system at

the data network level, e.g. use of firewall systems, etc. Indeed, the NGSCB project points to the exact trust solution explained below in that it attempted to put a “PINPad” directly into the structure of a PC workstation.

What more can be done to increase trust and confidence in online transactions?

Solution 2: PINPad – THE Proven and Trusted Solution (EFTPOS in Australia)

- Home/SME/user “PINPad” unit for transaction verification and prevention of identity theft.

Proposition:



Software add-on solutions to PC security have reached the end of any reasonable protection scheme for commodity PC based systems. The Australian, State and Local Government entities, in combination with the relevant industries and service providers, must cooperate in the purchase and integration of suitable “PINPad” sub-systems for use with end-user computer systems connected to the NII. These units will

make use of existing and planned magnetic strip and chip cards in the possession of users to secure transactions on an end-to-end basis. The sub-system will also be made available for use by the private sector, particularly for internet based banking and finance, health care and allied applications. Economies of scale will mean that the cost of these units will be small, and may even be, as per the situation with mobile phones, bundled into service agreements.

EFTPOS Led the Way in Trust:

The use of a PINPad for the generation and processing of electronic transactions by enterprises and end-users alike is well known, understood and trusted. Indeed, it can be argued that the success of EFTPOS in Australia and the public’ overall trust in the system, can be readily attributed to the development, standardisation and deployment of the PINPad structure. The standard cash register was considered, in the late 1970s and early 1980s, as unsuitable and insecure for the development of a national, trusted EFTPOS scheme alone. The introduction of both the PINPad, at the customer end of the system, and the “*Security Control Module (SCM)*”ⁱⁱⁱ at the financial transaction authorisation end, enabled the

The computer and networks security add-on industry is an industry that simply should NOT EXIST, e.g. anti-virus software, firewall sub-systems and the like. A standard, secure computer system should simply not need them.

ⁱⁱⁱ Disclaimer: The author was the 1979 Founder, CEO and Technical Director of ERACOM Pty Ltd which, in Australia, researched, developed, manufactured, sold and supported SCM and allied cryptographic units on a worldwide basis. He left the company in 1998.

development and deployment of one of the most successful examples of the digital economy over the last 25 years in Australia.

The units will be made in Australia, supporting Australia's own ICT industry, and made available at cost to Australian citizens by industry and governments alike. Integration with all basic systems currently in use, including any network based protocols etc. such as those for EFTPOS, healthcare, etc., will be the subject of a DBCDE contract to the ICT industry and DBCDE will create and maintain a group dedicated to the propagation of use of this unit. Connection will be available for a minimum of both Intel Corporation based PCs and Apple MAC systems operating under Microsoft Windows or LINUX/BSD operating systems and Apple MAC OS/X etc. the unit will be made available under all current browser systems with a fully OPEN and available application / system programming interface specification and software library set.

The underlying encryption system, and its allied key management and PKI structure, will be approved by the relevant Australian Government organisation, the Defence Signals Directorate (DSD). The unit will be subject to evaluation under the appropriate Australian Government approved scheme, the AISEP. The unit will be evaluated at least at Common Criteria EAL4+ level with the underlying cryptographic subsystems and embedded operating system at a higher level. A level of at least EAL5/6 is suggested for the cryptographic sub-system.

An "Inconvenient" ICT "Truth".

Principle:

It is unreasonable for Governments to state or imply that the PC, mobile phone or personal digital assistant (PDA) or the like are suitably secure and trustworthy devices for safe and secure electronic transactions without notable hardware and software modifications at the ICT industry level. These have been recommended by the ICT industry as well as by leading consultants, advisors and researchers in the area, over the last 10 years or more, such as by use of the "PINPad" or similar products and systems.

Indeed, it is essential that government ensure that those individuals and enterprises who assess that the current risk involved in use of the "*digital economy's*" structures is too high, for the present and without substantial security upgrade, will have access to alternative service provision, e.g. the banking and finance industry offers sufficient branch and similar services to meet customer demands in a reasonable way.

Portraying Unwarranted Confidence versus Real Assessment and Honest Disclosure:

This brings into debate the political and public policy challenge of taking approaches that have the effect of potentially decreasing confidence in the underlying structures of the digital economy versus making the facts, evidence and risks involved available to the public. This debate is resonating in the current economic "meltdown" situation

but leading politicians have opted for the latter approach^{iv}, i.e. it is essential that the public is NOT misled about the realities facing the nation. Indeed, Queensland's State premier, the Hon A Bligh, uses the rhetoric of a "war footing" to describe the situation.

Queensland's State
Premier, the Hon A
Bligh



Likewise, it is totally unbalanced for governments to advocate, through various documents, websites, publicity campaigns and the like, that information security responsibility belongs solely to the end-user. Any such statement can only be based on some perceived and hopeful statistical unlikelihood of transactions being compromised rather than any real, technological solution to the problem or acceptance of security responsibility by the ICT industry and owner/operators of information systems for numerous applications. Such statistical observations are subject to extreme variations worldwide and over time.

The home/SME, and indeed any application of a personal computer, connected to the global Internet cannot offer, by itself, a proven secure platform for the development of a digital economy. The PC, and allied "nodes" based on such commodity products, cannot be assumed to be "suitable for safe and secure electronic transaction" usage at any level and particularly not for those governmental transactions aimed at increasing ease of access of the citizen to public sector services and where privacy is a critical factor along with any assessment of the risk of "identity theft". Software based sub-system usage, where such systems are offered by enterprises that do not normally offer the basic computer system, has been proven to be ineffective in many cases, offering only a basic level of protection. The requirement of the end-user to continuously "patch" and update their systems is unreasonable and actually proven to be ineffective.

- **Special Note: "Dial-up Disaster"**

For those forced, or opting, to use "dial-up" Internet connections, such updating is actually infeasible. These users cannot reliably or conveniently download appropriate "patch" software packages or even efficiently maintain such subsystems as virus signature databases, etc. This may continue for an unacceptable time in regional and fringe city areas where such telecommunications as multiplexing, "pair-gain" and like technologies have been deployed in the basic telecommunications infrastructure and there appears to be no intention of their replacement by commercial operators.

^{iv} Qld on economic war footing: Bligh : Published 3:30p.m. 26th January 2009
By Tony Bartlett : Updated 4:09p.m. 26th January 2009

Queensland cabinet ministers have been warned the state is entering 2009 on an economic war footing. Premier Anna Bligh says a lengthy briefing from Treasury on the state of Queensland's economy will dominate Tuesday's first state Cabinet meeting of the year. "I want every minister to understand the environment we're going into, and their responsibilities in responding," she said. "It will be a very lengthy briefing from Treasury about the current state of the Queensland economy, the Australian economy, and what's happening in world markets that affect our producers and our markets and industries."
Source: <http://www.thedaily.com.au/news/2009/jan/26/aap-qld-on-economic-war-footing-bligh/>

The PC and PC based server nodes were never developed with security foremost in the program of development. The very existence of the so-called “anti-virus” and information security “add-on” industry attests immediately to the basic unsuitability of the PC for transaction usage. Moreover, no computer application can be any more secure than underlying “middleware”, libraries, operating system or allied structure.

Evidence (General):

- a. Increased sophistication of “malware” and its rapid propagation over the Internet is now at such a state that the average user, home or SME, cannot reasonably maintain any so-called software security package “add-on” to the PC.
- b. The average user does not have the education, training or ability to recognise, diagnose and correct attacks on the computer system.
- c. Modern attacks on the end or server / node systems do not necessarily require the user to perform any overt action, with penetration occurring through normally accepted actions, such as “Web surfing”.
- d. Total compromise of the PC platform has now reportedly reached alarming proportions, i.e. the use of so-called “Zombie” systems in large scale “botnets”.
- e. Compromise will become easier, and less observable by the ordinary user, as high speed broadband data communications services become available to all Australians.

Solution 3: ISP Administered and Operated Identity Based Cryptography.



NEHTA represents the best example in the near future for the use of modern identity based encryption (IDE). The use of cryptographic system has long represented the only real way to provide privacy, integrity and authenticity services in a telecommunications network environment. However, end users are totally inexpert in the associated but vital area of cryptographic key management.

Action:

DBCDE will examine and report on the potential for identity based encryption schemes, with associated key management administration at the ISP or equivalent levels, for the enhancement of security in the digital economy.

Solution 4: Data Breach Notification Law.

The DBCDE Minister must immediately promote the drafting and submission of ALRC data breach notification style legislation. This would demonstrate to Australia, and particularly to both public and private enterprises, that the Rudd Government is serious about overall information privacy and the building of confidence in the digital

economy. At a time of economic recession the temptation for both the public and private sectors will be claim lack of sufficient budget to support effective privacy and security functionality and enforcement in information systems. This risk must be understood and countered through leadership in the public sector.

The following quotation gives an example of reported commentary from the USA.

Wall Street Journal : September
9, 2008, 12:08 am
**Why All the Data Breaches?
Businesses Just Don't Care**



U.S. businesses reached an ignominious milestone in August, when the number of data breaches disclosed publicly for the first eight months of 2008 already surpassed the total number of disclosed breaches for all of last year.Cyber criminals are adopting more sophisticated techniques for breaking into businesses; businesses are creating, storing, and sharing more data than ever before; and employees don't understand the value of the data that they work with or the myriad ways the data could fall into the wrong hands...

*Schneier says that what is happening in the tech-security world is a **market failure similar in nature to what has happened with global warming**: There is a problem that everyone is contributing to, but individual businesses don't have a reason to do anything about it. The only way that security will improve, says Schneier, is **if the government creates an incentive**, either by allowing individuals to hold businesses liable for data breaches or by introducing regulations that impose criminal or stiff civil penalties on businesses that experience a breach. "If the penalty for not complying is nothing why would you comply?" he says.*

What is needed to address the SME concerns identified above?

Solution 5: An Australian Government Lead with Hardened Server Systems – Compulsory Requirements

- Trusted system usage for public sector server nodes.

Proposal:

Use of AISEP evaluated systems will be **mandatory** for all information systems developed and operated by the Australian Government and its agencies where security and privacy of information, particularly personally identifiable information, is present. This requirement will also extend to all ICT contractors / outsourcing operators. AGIMO will determine, in conjunction with DSD, the appropriate "profile" needed to meet the security requirements of any particular public sector information system and network.

The Australian Government will move towards the use of AISEP designated and based systems for all servers as information systems are enhanced and/or updated. In particular the Australian Government will seek the advice of the Defence Signals Directorate in designating the appropriate security "profile", from the agreed set of security profiles under the Common criteria recognition Arrangement (CCRA) to which Australia is a signatory, for each and every governmental information system

that is operated, developed or planned for interconnection onto the Internet for use outside restricted data communications networks.

Are there possible barriers preventing a strong online retail experience in Australia? What can industry and other stakeholders do to address these?

The PINPad suggestion above solves these problems and would build upon the accepted and trusted retail experience by all.

What is the experience of business-to-business e-commerce in Australian supply chains? Are companies (large and small) saving money because they are now making electronic transactions? What are the barriers to take-up? Are international companies benefiting from e commerce transactions with consumers and with other businesses?

No comment.

What evidence shows the possible barriers preventing greater online content offerings? What can be done to address these?

Proposal: Eliminate “Download Limits”

“Download limits” must be mandatorily removed by legislation for the Internet to become a real medium for the digital economy.

Evidence:

Australian ISPs set so-called “download limits” on users of the Internet in situations where the end user has little to no ability at all to control or even monitor such usage. Moreover, data “quantity” downloaded to a user’s system may be actually uncontrollable by them as such structures as advertising video clips, sound files and the like are force loaded into the user’s system from the server end. In any reasonable commercial transaction an inexperienced, novice user should not be expected to pay for advertising they do not need or want nor be unable to determine just what charges they are responsible for.

From the ISP/carrier viewpoint this limit is argued on the basis of “rationing a scarce resource”. However, in many cases it can also easily be recognised as a further profit “gauging” activity as so-called “excess megabytes” of downloaded material are charge at a much higher rate, e.g. 15 cents per megabyte, etc. A press report re this matter is appended to this submission under the title “*Gamer Hit with \$6,000 Bill*”.

Theme:

The single main barrier to usage of the Internet for advanced online content delivery is the imposition of so-called “download limits” over which the end user has little control. In the case of “streaming media”, such as Internet radio, TV, cooperative game playing and the like, this technique is totally counterproductive.

Proposal: No “Throttling” - Open and Equal Access

So called “throttling” of Internet or allied data communications speed or services on the basis of commercial or other arrangements will be outlawed and the Minister will develop appropriate legislative instruments to enable this to become law in Australia.

Theme:

Open and equal access to the Internet and allied data communications services, must remain equitable and known by both ISPs, common carriers and the end-user alike.

FURTHER EVIDENCE:

Evidence Bases for Proposed Solutions and Observations:

a. Applications cannot be secure if the underlying systems are not – USA, National Security Agency. – 1998 / over 10 years ago

Source: USA'S National Security Agency (NSA)

The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments

by

Peter A. Loscocco, Stephen D. Smalley, Patrick A. Muckelbauer, Ruth C. Taylor, S. Jeff Turner, John F. Farrell (National Security Agency)

Proceedings of the 21st National Information Systems Security Conference, pages 303-314, October 1998.

Although public awareness of the need for security in computing systems is growing rapidly, current efforts to provide security are unlikely to succeed. Current security efforts suffer from the flawed assumption that adequate security can be provided in applications with the existing security mechanisms of mainstream operating systems. In reality, the need for secure operating systems is growing in today's computing environment due to substantial increases in connectivity and data sharing. The goal of this paper is to motivate a renewed interest in secure operating systems so that future security efforts may build on a solid foundation.

The computer industry has not accepted the critical role of the operating system to security, as evidenced by the inadequacies of the basic protection mechanisms provided by current mainstream operating systems. The necessity of operating system security to overall system security is undeniable; the underlying operating system is responsible for protecting application-space mechanisms against tampering, bypassing, and spoofing attacks. If it fails to meet this responsibility, system-wide vulnerabilities will result. The need for secure operating systems is especially crucial in today's computing environment. Substantial increases in connectivity and data sharing have increased the risk to systems such that even a careful and knowledgeable user running on a single-user system is no longer safe from the threat of malicious code.

b. Microsoft Inc.

In 2005 Microsoft Inc. proposes use of PINPad style unit for secure transactions.
Summary: PC is unsuitable as it exists – separate device needed.

Dave Steeves -
dsteeve@microsoft.com
Security Software Engineer
Microsoft's Security Business
& Technology Unit
System Protection Products
Team.
at

1st TIPPI Workshop
Trustworthy Interfaces for Passwords and Personal Information
Date: June 13th, 2005
Location: Stanford University,

Securing Online Transactions Recap

- Current Online Transaction Models
 - Threats Still Exist
- Solution
 - One Time Secret per Transaction
 - Keep Secret Off Untrusted Device
- Reduces Attack Surface
 - Attack vectors localized
 - Hardware Hacking/Physically Present
 - Tempest Attacks
 - Break Crypto

Comment:

A representative and IT professional of THE major supplier of basic PC operating systems and allied software agrees that a PINPad type device is necessary. This cannot be easily contradicted by others who do not design and distribute such basic ICT systems as a computer's operating system.

c. TPM 1.2

See URL <https://www.trustedcomputinggroup.org/specs/TPM>



The "Trusted Computing Group (TCG)" exists to clearly demonstrate that hardware security is an essential part of any program to secure cyberspace. Its website clearly states as follows, at 30 January 2009.

About the Trusted Computing Group

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specifications will enable more secure computing environments without compromising functional integrity, privacy, or individual rights. The primary goal is to help users protect their information assets (data, passwords, keys, etc.) from compromise due to external software attack and physical theft.

The TPM 1.2 hardware module and supporting software system is a start upon the direction outlined under the PINPad solution mentioned above, However, the TPM DOES NOT offer a trust path between the keyboard, mouse or other input devices and similar output units such as screens, printers, etc. which must be supplied by

other hardware designs and implementations in the PC unit itself. The very existence of the TCG is real evidence that new policies are needed related to the e-security obligations of the IT industry.

d. Trust and Confidence.

A 12 week perusal of public statements by members of the add-on ICT security industry give any amount of evidence that the battle against malware has largely been lost in relation to general purpose microprocessor based PC systems in common usage. In addition, sophisticated techniques are well beyond the detection capability and understanding of the ordinary user.

i) Kaspersky – 27 Jan 2009 ; The Australian.

Crime pays and so does anti-crime software
Karen Dearne | January 27, 2009



We are here to bear witness to a very big change in the dimensions of cybercrime, Kaspersky says. We are now locked in an inevitable cycle of technological escalation, an arms race that can only be continually fought, and perhaps never conclusively won. "Cybercriminals are organised, motivated and increasingly professional, and their attacks are both more numerous and sophisticated," Kaspersky says. "We don't have hard data, but it would be no surprise if online crime revenues reached \$US100 billion this financial year.

"That's placing a very high load on global economies, but still governments don't see it because it's on the internet, it's hidden in the cloud. It is also placing a very high load on protection technology, both within the lab in terms of capture and analysis, and in the product, in terms of fighting malicious applications and the use of computer system resources." The growth of malware is huge: in 2007, at least five new samples emerged on the internet every two minutes. Today, new malware samples appear every two seconds, according to Kaspersky. While there were about 2 million malware variants circulating in 2007, this year the total will reach some 15-20 million samples.

"The antivirus industry is in panic," Kaspersky says. "It's not possible to process all these samples with the old manual techniques that took days to analyse and respond. Now we are in an era of automatic malware processing systems."

ii) FBI / USA

FBI warns of cyber attack threat

Sydney Morning Herald - January 7, 2009 - 2:23PM

Cyber attacks pose the greatest threat to the United States after nuclear war and weapons of mass destruction - and they are increasingly hard to prevent, FBI experts say. Shawn Henry, assistant director of the FBI's cyber division, told a conference in New York on Tuesday that computer attacks pose the biggest risk "from a national security perspective, other than a weapon of mass destruction or a bomb in one of our major cities."

"Other than a nuclear device or some other type of destructive weapon, the threat to our infrastructure, the threat to our intelligence, the threat to our computer network is the most critical threat we face," he added.

US experts warn of "cybergeddon", in which an advanced economy - where almost everything of importance is linked to or controlled by computers - falls prey to hackers, with catastrophic results. Michael Balboni, deputy secretary for public safety in New York state, described "a huge threat out there" against everything from banking institutions to water systems and dams. Henry said terrorist groups aim for an online 9/11, "inflicting the same kind of damage on our country, on all our countries, on all our networks, as they did in 2001 by flying planes into buildings." A web attack of that scale has not yet happened in the United States but computer hacking - once something of a sport for brilliant delinquents - is rapidly evolving around the world as a weapon of war.

SOME REFERENCES USED:

Libicki, M C et al

Scaffolding the New Web : Standards and Standards Policy for the Digital Economy,
Rand Corp. USA 2000, ISBN/EAN 0-8330-2858-8

Utimaco Safeware AG

“Shifting data Security Boundaries: Call for new Strategies”

Available at URL <http://www.utimaco.com>

Shari Lawrence Pfleeger, Daniela Golinelli, Robin Beckman, Sarah K. Cotton, Robert H. Anderson, Anil Bamezai, Christopher R. Corey, Megan Zander-Cotugno, John L. Adams, Roald Euller, Paul Steinberg, Rachel Rue, Martin C. Libicki, Michael Webber
Cybersecurity Economic Issues : Corporate Approaches and Challenges to Decisionmaking

Rand research brief, 2008

Available at URL <http://www.rand.org>

Martin C. Libicki

Conquest in Cyberspace : National Security and Information Warfare

Cambridge University Press, ISBN-13: 9780521692144

SOME SOURCE MATERIALS:

Theme: growing loss of confidence in the USA.



Security - MetaData: The Rising Price Of Data Breaches

Andy Greenberg, 02.02.09, 12:00 AM ET

More bad news in the world of data security: Companies aren't just losing more of their customers' private information than ever before. **Customers are also losing patience with those increasingly common breaches.**

According to a report released Monday by the Ponemon Institute and funded by encryption firm PGP, the cost of a data breach for companies has risen to \$202 per lost record, up from \$197 in the institute's 2007 study. For the 47 companies audited in the study, those costs added up to \$6.6 million per incident.

A growing portion of that financial hit comes from angry or distrustful customers. While data breach costs for detection, notification of victims and credit monitoring services all fell during the last year, the cost of lost business grew to an average of \$139 per company from \$128 in 2007, as customers stopped dealing with businesses they considered negligent with regard to data security.

The rising impact of data breaches may reflect the growth in the sheer volume of publicly reported data breaches in 2008, dramatically more than the year before, according to data tracked by the Identity Theft Resource Center. In 2008, 646 breaches were reported, up from 446 in 2007. The turbulent financial industry was especially affected: More than half the records lost in 2008 came from banks and financial services, up from 7% the year before. (See "Banking's Data Security Crisis.")

According to the Ponemon study, those bank breaches may be even more costly than the average. While 3.5% of customers typically abandon a company that's experienced a breach, 5.5% of customers flee from financial services companies after a data loss incident. The health care industry shows the highest cost of lost business, with 6.5% of customers abandoning a breached company.

"Businesses that depend on a strong sense of trust have to be especially careful," says Larry Ponemon, founder of the eponymous research group. "They're on a high pedestal, and they experience a much harder fall."

That may be an especially sobering thought for Heartland Payment Systems,, which revealed two weeks ago that it had been the victim of a hacking incident that siphoned off credit card numbers from its network. Given that the company processes 100 million transactions a month and hasn't yet revealed the duration that its network was compromised, the breach may be the biggest--and the costliest--of all time.

Source:

http://www.forbes.com/2009/01/30/security-hacking-enterprise-technology-security_0202_data_breach.html?partner=alerts

Accessed at 2 Feb 2009.

Theme: Bias to One ICT System Supplier.

Macs, Linux to wait as ATO tenders e-tax

By [Suzanne Tindal, ZDNet.com.au](#)

December 01, 2008

URL: <http://www.zdnet.com.au/news/software/soa/Macs-Linux-to-wait-as-ATO-tenders-e-tax/0,130061733,339293572,00.htm>

The Australian Taxation Office (ATO) last week put the contract to maintain and develop its e-tax system out to market, with indications remaining that Mac OS X and Linux versions of the software are a ways off.

.....The selected contractor would need to work on the server infrastructure and client application components of the 2009 e-tax system to result in the 2010 version, which has to be operational by 1 July 2010. The changes will involve including the 2010 system legislative changes which are required by the Tax Office.

Local IT services firm DWS Advanced Business Solutions has held the e-tax contract until now. The company will work together in a transition period with whichever firm wins the e-tax contract up for grabs. DWS CFO Lachlan Armstrong said that the company definitely intended to rebid for the contract.

The software for the e-tax system has been written in a mix of Delphi, VB, C++, C# and VB.NET, with the user application being mainly in Delphi, which the ATO would like to maintain.

The w-tax user application is currently able to be run on computers running Windows 2000 Professional Service Pack 4, XP Service Pack 2 (32 bit) and Vista Service Pack 1 (32 bit).

The tender documents expressed that tweaking the e-tax system so it could be used on alternate operating systems was still on the agenda, however when *ZDNet.com.au* contacted the tax office, a spokesperson said that getting the system working for non-Windows operating systems was not a mandatory requirement, only "identified as a consideration".

The spokesperson also said that the ATO had not determined which operating systems it hoped to target.

The ATO said in [March 2007](#) that it intended on making the system workable for non-Windows operating systems such as Mac and Linux, promising a trial in 2008 and a new product rollout in 2009. However, the program encountered "significant challenges and complexities", according to the ATO spokesperson, which has meant the trial has been indefinitely delayed.

Theme: Download limits – hinder the digital economy.

Gamer hit with \$6000 Bigpond bill

Stephen Fenech | *January 21, 2009*

WHEN Justin Cavanagh decided to play online games with his mates over the Christmas break he didn't realise his actions would cost him thousands of dollars.

Mr Cavanagh, 29, connected three computers at his North Gosford home so his friends could go head-to-head on the popular online World War II strategy game Battleground Europe.

But he exceeded his Telstra Bigpond 60GB ADSL2+ plan by more than 38GB.

Telstra's policy is to charge excess data at a rate of 15c per megabyte but, the company says, Bigpond customers are always sent email notification when they are nearing their download limit.

When Mr Cavanagh's next Telstra bill arrived it said he owed them \$6041. A distraught Mr Cavanagh contacted Telstra about the massive bill and was told to send an email.

"It was a bit hard to send an email because they cut off my connection," he said.

When *The Daily Telegraph* contacted Telstra a spokesman rang Mr Cavanagh immediately and said the bill would be waived as "a gesture of good will".

The Daily Telegraph

(Source URL <http://www.australianit.news.com.au/story/0,24897,24942175-5013041,00.html>)

Theme: 1 Trillion US Dollars of Loss per Annum – Problem of Intellectual Property Protection in the Digital Economy

McAfee, Inc. Research Shows Global Recession Increasing Risks to Intellectual Property

Businesses Lose More Than \$1 Trillion in Intellectual Property Due to Data Theft and Cybercrime

DAVOS, Switzerland--(BUSINESS WIRE)--McAfee Inc. (NYSE:[MFE](#)) today announced findings from the first global study on the security of information economies. In the study, *Unsecured Economies: Protecting Vital Information*, security experts and senior IT decision makers warned that the global recession is putting vital information at greater risk than ever before. The results were reviewed by McAfee's Cybersecurity Experts Council, announced separately today.

Researchers from Purdue University's Center for Education and Research in Information Assurance and Security examined responses from more than 800 CIOs in the United States, the United Kingdom, Germany, Japan, China, India, Brazil and Dubai. The research examined where vital information such as intellectual property originates, where it is stored globally, how it is transferred and lost. The companies surveyed estimated they lost a combined \$4.6 billion worth of intellectual property last year alone, and spent approximately \$600 million repairing damage from data breaches. Based on these numbers, McAfee projects that companies worldwide lost more than \$1 trillion last year.

"Companies are grossly underestimating the loss, and value, of their intellectual property," said Eugene Spafford, professor of computer science at Purdue University and executive director of CERIAS. "Just like gold, diamonds or crude oil, intellectual property is a form of currency that is traded internationally, and can have serious economic impact if it is stolen."

"Based on the survey findings McAfee conservatively estimates that the global damage from data loss to top one trillion dollars," said Dave DeWalt, president and chief executive officer of McAfee. "This report is a wake-up call because the current economic crisis is poised to create a global meltdown in vital information. Increased pressures on firms to reduce spending and cut staffing have led to more porous defenses and increased opportunity for crime. Companies need to stop looking at security as a cost center but as a business enabler."

The McAfee Unsecured Economies report suggests that the ability to safely store intellectual property is a key driver of security investment in Brazil, Japan and China. Sixty percent of Chinese respondents cited "safer storage" as a reason for storing intellectual property and other sensitive information outside of their own country.

Key findings:

Recession puts intellectual property at risk

Organizations are clearly worried about the global financial crisis and its impact on the security of vital information like intellectual property. Thirty nine percent of respondents surveyed believe vital information is more vulnerable in the current economic climate than before.

Commitment to protecting vital information varies

Developing countries are more motivated and spend more on protecting intellectual property than their Western counterparts. Brazil, China and India spent more money on security than Germany, UK, US and Japan. Seventy four percent of Chinese and sixty eight percent of Indian respondents invested in securing their intellectual property for competitive advantage.

Intellectual property is now an international currency

An emerging target for cybercriminals is intellectual property, and experts say there has been an increase in the number of corporate data intrusions by organized cyber mafia gangs. Cybercriminals are increasingly targeting executives using sophisticated phishing techniques. The biggest concern for thirty nine percent of respondents was protecting their intellectual property from outside data thieves.

Employees steal intellectual property for financial gain and competitive advantage

An increasing number of financially challenged employees are using their corporate data access to steal vital information. As the global recession continues and legitimate work disappears, desperate job seekers or “cyber moles” are stealing valuable corporate data, which may be seen as desirable by potential future employers, to make themselves more valuable in the job market. Forty two percent of respondents said displaced employees were the biggest threat to vital information.

Geographic threats to intellectual property

Geopolitical perceptions are influencing data policy reality. China, Pakistan, and Russia were identified by companies surveyed as trouble zones for various legal, cultural and economic reasons. Twenty six percent of respondents purposely avoided storing intellectual property in China. Yet forty seven percent of Chinese respondents believed the United States posed the biggest threat to their intellectual property.

The report concludes with suggested best practices for protecting valuable digital assets, not only in order to survive—but to thrive—in these challenging times. For a full copy of the report *Unsecured Economies/Protecting Vital Information* please visit <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.

(Source: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>)