SUBMISSION NO. 68

Submission to

House of Representatives

Communications Committee

Inquiry into Cybercrime

November 2009

Web Management InterActive Technologies Pty Ltd
P.O. Box 1073, Capalaba, Qld, 4157
Voice Phone: 07-3823-5150
Fax Phone: 07-3823-5152
Email: info@wmit.net

Proposal for an Australian Protected Network

Strategic Solutions Summary.

- **What is the Problem?**

  a. Criminal elements have virtually free rein in the Cyber world.
  b. The vast majority of people have inadequate protection or none at all.
  c. Existing solutions are largely *reactive* in nature.
  d. There is resistance to use of technology due to fear of attack.
     & total innocence of users to the real risks of attack.

- **What is the Solution?**

  a. Education; and that includes supporting users with information.
  b. Improved security surrounding transaction based activities.
  c. Greater dissemination of protection products into the community.
  d. The Australian Protected Network.

What is the Australian Protected Network?

The Australian Protected Network throws a protective mesh around the equipment that is connected to it. Long before a cyber-criminal's Internet packet can attack a piece of equipment, it is stopped cold. Put simply, that's all there is to it.

It provides something that should have been there from the start.

It provides: Control.

Ladies and Gentlemen, we are at War. And the battle is raging on many fronts at the same time. Botnets are threatening us from inside and outside our country. Viruses and Trojans threaten our information pathways. The Firewalls of our major institutions are continually battered by an unrelenting enemy who has virtually unlimited power in this space. And all the time, sinister forces plan and plot to overcome our strongholds, invade our privacy and steal whatever they may. And those most at risk are also those who are most vulnerable. The young from bullying tactics and the elderly who, with fear and trepidation in their hearts, are unwilling to risk using the internet.

Sound dramatic? Yes. But it's true. While I was writing that, my own firewalls were battered by attacks from inside the Chinese continent. Probably from compromised machines. Next there was an attack starting from Italy. It's always moving and changing. We must do something about this. And we must do something NOW. The time for ignoring it and hoping it will simply go away is over; we need to make a stand and show that we will protect ourselves.

e) Future initiatives that will further mitigate the e-security risks to Australian internet users;

f) Emerging technologies to combat these risks.

The **Australian Protected Network** consists of;

1. A hardware/software component in the form of a Firewall/Proxy server. (Simple Linux boxes running the common Squid proxy server for example)

2. A centralised database system which receives input about threats and programs the Firewall/Proxy server. This Computer Operating on Resource Advantage determines things to block based on security levels ***the users choose***, and updates the Firewall/Proxy server.

3. * YOU *

The Australian Protected Network operates as a central point for reporting and blocking of threats as they appear. This is a living system which grows and changes along with our requirements. The C.O.R.A. system actively seeks out threats guided by a hierarchy of members of the Australian internet community. One of the problems with threats is that they are constantly evolving. Attacks come from different directions all the time. Our system extrapolates likely vectors for the next location of a threat, and seeks to prevent it.

This system puts the future of Australian internet users back in their hands. Once threats have been identified, we can actually take some “proactive” action against them.

The majority of domestic users only have simple needs when it comes to the internet. They simply want to be able to send and receive emails, while checking the news and weather. They want to be able communicate with their mates and surf safely on the net. With the maximum amount of protection turned on, they’ll be able to do this inside a protected network which is free from external attack.

There are still other ways that cyber criminals can operate, and other measures such as Education and E-Security awareness that are of paramount importance. We must ensure that people are educated in the ways of Cyber Safety, and that Anti-Virus and Internet Security measures are installed on as many network connected devices as possible. Towards that end, the operations of the Australian Protected Network are bound together in an InterActive Information Window which provides a communication centre for people on the network. It works as a secure method of disseminating information to the network community.

The Australian Protected Network designed by Web Management operates as a first line of defence in this war on Cyber Terrorism. We truly do live in the “lucky country”. The freedoms we all enjoy are not available everywhere in the world. The health system that we complain about is just fantastic compared with other countries. When this network comes online, our Internet access will be the safest in the world. We will be the envy of other major governments, and they’ll be wanting to set up similar protection themselves.

Our design is unique in so many ways. One point of concern that arises with other systems is that of Net Neutrality or Restriction of access without people’s knowledge. Enter the Australian Protected Network. All functions and operations are open to the users and the sites involved. Users are able to choose the level of protection they want to have on their access. Sites are able to see how the network is affecting their traffic and if they need to do something to correct any issues. This negates any concerns of faceless people surreptitiously blocking things without cause.

With the introduction of the Australian Protected Network –

- Some aspects of Internet crime will drop overnight. Unsecured routers and embedded devices behind the protected network may still be compromised by drive by data thieves, but they are primarily using them to download illicit materials. If those materials aren't made available through them, then they won't have a motive to go after them in the first place. Any devices which are infected will be locked off from the rest of the network, so any collateral damage will be limited.

- Instantly, the majority of known compromised web site linked Viruses will lose their ability to report back to their criminal masters. This will render them virtually inert as long as the device remains behind the protected network.

- ISPs (Internet Service Providers) will no longer be powerless to prevent criminal activities such as theft of copyright materials through their network. ISPs that may be at risk of prosecution for allowing their network to be used for the transfer of copyright material will be protected from prosecution because sites which promote copyright material theft can be blocked. They will have done all that is possible to prevent breaches just by having the Protected Network available.

- Searching for criminal activity on the Australian internet is currently like looking for a needle in a haystack. With domestic access behind the Protected Network, it will become like looking in a hay bale. I'm not saying it will be easy, but it will certainly make the job of find criminal activity much easier.

- There will be greater uptake of internet based technologies. Consumers will have a first line of defence and be educated through the InterActive window of what they can do to be Cyber safe.

- The InterActive window will also serve as a first point of warning against emerging threats on the internet. Security alerts and warnings from banking institutions, etc. can be relayed through the InterActive window.

- Before any site is blocked the person blocking that site has the opportunity of connecting with the webmaster (usually via a link at the bottom of a webpage) to leave a message indicating the reason the site will be blocked. Those writing such messages will be contacted through the system so the site can be made active when the issue is sorted out. Sites, particularly Australian run sites because of our connection to them, will be registering their web sites with the system. Some protection measures will need to be put in place to prevent them taking any punitive actions against individuals or the network, but there will be ample recourse for them to correct any problems and get their site reinstated.

- This system takes decisive action about the problem of compromised websites, and operates alongside such systems as the Australian Internet Security Initiative, from whom we would of course welcome input. The Australian Internet Security Initiative has links to ISPs in Australia and is able to effect some change on the face of the Internet in Australia. The Australian Protected Network will take it a step further by being actively involved in protecting the nation as well as being able to inform the site.

- Privacy is of a great concern to Net Citizens, and Australian Net Citizens are no different. Unlike other systems which monitor access through their products, the Australian Protected Network design does NOT use the Proxy logs or monitor their traffic at any stage of operations. Only the user access through InterActive Window gives any feedback into the system, and this is totally manageable by the user.

The Inner Workings.

The technology and operations behind this are involved and complex, but the following is a précis of operations to help you better understand Web Management's technologies, and its role within the operations of the Australian Protected Network.

The actual Firewall technology we are going to use may vary, but the principle will remain the same. Information is passed around the Internet using protocols which different devices have in common. Internet Protocol addresses are often called IP Addresses for short. Information Packets are transferred from IP address to IP address in a cooperative manner across the Internet.

Now let's say that we know that a particular IP Address is home to a Criminal attack upon our IP Address. Between our IP Address and their IP Address we place a "Firewall" IP Address. When the Firewall receives the packet from the offending IP Address, we reject it, because we know that we don't want that packet.

The same thing happens with the Proxy server which is running on the Firewall machine. It receives a request to connect to an offending Web Address on the World Wide Web. We reject the attempt to connect, since we know that the connection is a bad place to connect to.

That is the simplest way to describe how the system of protection works on the ground. Now: How do we decide where and with whom we don't want to make connections?

In late 1984, James Collins developed a system for linking information together, which was quite simply a revolutionary way of thinking. That system and method of data storage and retrieval is what makes it possible for the creation of the technologies which run Web Management today. It works in such a way that once a given piece of data has been analysed, the very concept of it is stored in a database and it becomes part of a whole. This information becomes part of a vast array of information which builds with each successive addition.

As time passes, the information coalesces and develops into new information, and can then be transformed by both inner and outer influences to form new patterns. The expression of these patterns is what drives all the Web Management technologies, right down to the production of Web Sites and the production and targeting of information for users. It literally produces the results a customer wants before they are even aware that they require it. And it does all this while maintaining the user's security and privacy. The only information Web Management InterActive Technologies gets from the user is that given freely through the InterActive Window, and that information is fully visible and manageable by the user themselves! There is NO monitoring of user activities on the network and unlike other systems there is NO following the user around the internet copying their details.

That, in a Nutshell, is how the InterActive Technology works. The capital "A" is there for a reason. Because the data is always active, always moving, and always in a state of flux.

We have deployed this system to work on the question of determining what threats exist out there in the Open Internet and it has been protecting people since 2003.

Should this proposal be adopted, we intend to include input from various additional sources. These might be external organisations that warn us of impending attack addresses, or Australian Government bodies which advise us of dangers. There will also be the input from the Australian public.

- Monitors are normal everyday users. They basically can either agree or disagree with decisions made by the system. Over time, the veracity of their input is gauged, and over time, they can reach the point where they are found to be trustworthy enough individuals to become Moderators.

- Moderators have varying security access to the system. The more accurate their input, the more sway they have over the operation of the system. It follows their lead, but still operates on the basic premise of its internal operations.

- Committee members are appointed to their position. They have the control of "Veto" over decisions and are drawn from experienced Web Management Staff and possibly external bodies such as Government officers. Their inclusion is important, to prevent imbalances that may occur.

This puts our future on a secure footing where we are able to quickly respond to threats as they appear, and actively seek out impending threats and neutralise their potential. We have a network of people who are interested and able to work towards the protection of our nation. We use the internet to do something that it has proven time and again that is amply able to achieve; that of collaboration to achieve a common goal.

The Future.

There is a lot more to do after this initial phase of implementation.

- Basic protection for our Emails. A level of spam protection that at least filters out known viruses must be considered as a second phase of the Australian Protected Network.
- Safer chat systems which leverage existing systems while making them safer.
- Products which include weigh stations for the scanning of files for threats as they are transferred from one user to another.
- Providing communication channels for emerging cyber-threats. Linking people and the information they need to handle the future.
- And of course international cooperation with their similar facilities. We may be an Island continent, but we have the resources of the world itself at our disposal.

As you can see, the application of this system is really very simple. The technology is sophisticated beyond anything available anywhere in the world, but the application for both ISPs and Users remains straightforward. This first line of defence is the only rational move in a Cyber world dominated by forces which would do us harm. The future is a lot brighter for everyone, when we have a firm foundation on which to build a secure networking future. The Web Management group of companies stands ready to take up this fight. We only need *your* support to achieve this goal, in the defence of our nation.

I thank you for your time today.

James Collins

Managing Director,

Web Management InterActive Technologies Pty Ltd.