SUBMISSION NO. 15

The NetChoice Coalition
Promoting Convenience, Choice, and Commerce on The Net

Level 6, Art Wall Building
13 Kirketon Rd
Darlinghurst NSW 2010
www.netchoice.org.au

NetChoice
Convenience
Choice
Commerce

26 June 2009

Ms Belinda Neal MP
Chair, House Standing Committee on Communications
House of Representatives
Parliament of Australia
Canberra ACT 2600

By email: coms.reps@aph.gov.au

Dear Ms Neal:

Re: Inquiry into Cyber Crime

NetChoice is pleased to respond to the *Inquiry into Cyber Crime* issued by the House Standing Committee on Communications following the referral by the Department of Broadband, Communications and the Digital Economy.

NetChoice is a coalition of trade associations and e-Commerce businesses, established in the United States in 2000. In 2008, at the request of local e-commerce companies, NetChoice established an Australian chapter.

NetChoice promotes e-commerce and the choice and the convenience it offers. When necessary, NetChoice fights threats to online commerce and promotes policies that protect internet innovation. NetChoice is fearless at exposing the anti-competitive agendas behind calls for more regulation of the internet. NetChoice also seeks to change legacy regulations that discriminate against online versus offline commerce.

We have a strong record of working with governments to draft laws that not only protect consumers, but also promote competition from and within the e-commerce channel. Our goal is to find workable solutions to internet challenges, rather than unrealistic regulations that often bring unintended consequences.

NetChoice welcomes the Inquiry placing the consumer at the heart of its deliberations on cyber crime. As advocates for e-commerce as a mechanism to improve consumer welfare, NetChoice is greatly concerned about the dead weight cost of cyber crime on e-commerce activity and, as importantly, how the perception of cyber crime slows the uptake of e-commerce.

Addressing the terms of reference

The Inquiry's terms of reference can broadly be summarised as this: what is the nature and prevalence of cyber crime (term a); how does it impact the economy (term b); how aware are consumers about the risks (term c); what counter measure are being deployed (term d); and what more can be done (terms e and f)?

This submission will address, to varying degrees, all of the terms of the Inquiry.

a) Nature and prevalence of e-security risks

Internet users face a dizzying array of e-security risks, including viruses, Trojans, spyware, phishing, pharming, password-stealing URLs, keylogging applications, and denial of service attacks.

IT security threats are more potent than ever. Attacks were once the domain of technically talented hackers who took intrinsic pride in taking down corporate networks and crashing consumers' PCs. Today, criminals exploit IT vulnerabilities for financial gain and hackers can disable websites of their political enemies. Perpetrators of cyber-attacks include individuals, hacker groups, terrorist networks, organised criminal groups, and even national governments. And Cyber crime has migrated beyond fixed technology to mobile phones and PDAs.

Victims of internet crime range from the individual to the mightiest of institutions. Bot networks (botnets) have been established by organised criminal elements to send phishing attacks, spam, and other online fraud from distributed locations around the world. These botnets leverage the power of their network to attack national government and banking systems through distributed denial of service (DDOS) attacks.

These botnets are globally distributed and constantly growing, which makes it very difficult for ISPs to block emails from getting to their customers. Moreover, when a DDOS attack uses these botnets, the targeted website cannot block queries originating from around the world without blocking legitimate traffic as well.

b) The implications of these risks on the wider economy

The implications of cyber crime risks on the economy are substantial and growing, because of the growing importance of e-commerce to the Australian economy, and how the incidence and perception of cyber crime can damage that growth.

There is significant data on the direct losses associated with cyber crime, and no doubt other submissions will provide this information in detail. A recent report by the Australian Institute of Criminology[1] estimates that security incidents were costing businesses up $649 million a year in 2007, with another $2 billion being spent on security measures.

What is more difficult to gauge is the opportunity cost associated with unrealised economic activity due to cybercrime scaring people away from e-commerce. Given the scale of e-commerce today, this opportunity cost is surely a multiple of the direct losses experienced.

[1] Australian Institute of Criminology (2009), *The Australian Business Assessment of Computer User Security: a national survey*, http://www.aic.gov.au/publications/rpp/102/rpp102.pdf

In 2007-08 e-commerce accounted for around $15 billon in spending according to IBISWorld, and will reach $21 billion by 2014, growing at over 5% per year. AC Nielsen data from a 2006 study puts Australia at number three for e-commerce in absolute terms in the Asia Pacific, and number one in the region on a per capita basis.

Whilst by these numbers, e-commerce is a relatively small proportion of today's Australian economy, it will inevitably grow substantially over the next decade. E-commerce has the unparalleled ability to spawn innovations, increase convenience, and generate price-cutting competition that will create new wealth, jobs and incomes and lift the quality of life for Australians. E-commerce is especially valuable during a recession, as it gives consumers greater access to discount prices and markets for used goods, while helping businesses reach customers outside of their local market area.

E-commerce will thrive only when consumers and suppliers have high confidence in online transactions. That is, when consumers feel secure from fraud, that their privacy is protected, and that their children are safe from predators. On the supply side, companies need simple and cost-effective ways to establish online stores and they need to be confident about receiving payments and fair competition.

c) Level of community understanding and awareness of e-security risks

In what may sound like a paradox, NetChoice believes there is both too little and too much awareness about e-security risks. On one hand, the community is bombarded with stories about cyber crime, which serves to make many fearful about engaging in e-commerce. But on the other hand, the inherent complexity of cybercrime issues means many in the community find it hard to absorb the information they need to know to safeguard themselves.

There has been limited research undertaken to quantify either understanding or awareness of e-security risks. Unisys[2] has been tracking Australians' perception of internet security over recent years, specifically how secure they feel in relation to viruses or unsolicited emails, and the security of shopping or banking online. Their latest index shows around one-third of the population is very or extremely concerned about these issues.

NetChoice encourages the Australian Government to further study the level of understanding and awareness of security risks. It would be helpful in ensuring that counter measures are properly targeted.

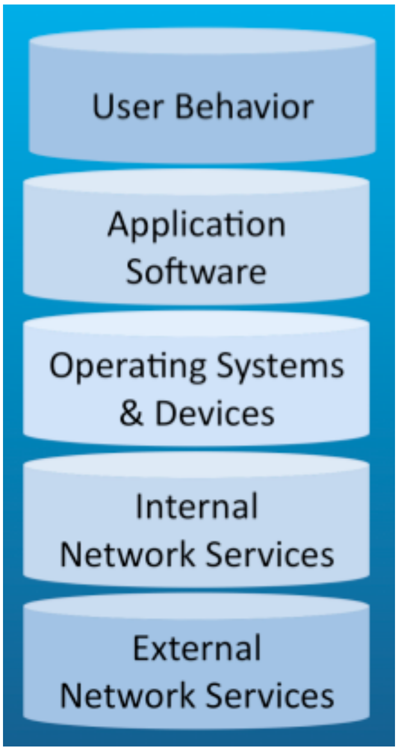
d) Measures currently deployed to mitigate consumers' e-security

Whilst confronting a complex problem or menacing threat, it is natural to search for a 'silver bullet' to slay the beast. But it is no surprise that we have yet to find the silver bullet solution for securing cyberspace. For instance, antivirus software is necessary, but not sufficient, to fully protect computers from viruses. An Internet firewall is essential for network protection, but not enough to secure an enterprise IT infrastructure. At the same time, blaming network infrastructure providers for all security problems neglects the overall complexity of cyber-security.

[2] Unisys (2009), *Australia Security Index,* www.unisyssecurityindex.com/australia/download-reports.asp

NetChoice proposes an alternative view. Cyber-security is best understood as a multi-layered stack where threats exist at multiple levels, rather than at a single point of failure. Today's computing and networking relies on highly interconnected systems of client and server-side software, plus PC and networking hardware – all managed by corporate, government, and personal users.

As seen in the figure at right, there are five primary layers in the security stack. (1) End-user; behaviour interacts with (2) application software that is installed on (3) operating systems and devices that all use network services that are (4) internal and (5) external to an organization.


User Behavior
Application Software
Operating Systems & Devices
Internal Network Services
External Network Services

For more on the security stack, please see our paper at http://www.netchoice.org/library/netchoice-security-stack-paper.pdf

Awareness campaigns are a necessary tool to effect end user behaviour, and an area where governments, law enforcement agencies and industry are rightly devoted substantial resources.

E-commerce firms are on the frontline of securing their customers, through detection and enforcement as well as through education of users. For instance, large teams of staff at eBay/PayPal, a NetChoice member, are dedicated to investigating online fraud, and the company offers a browser toolbar to help protect customers against fake copies of its Web sites.

e) Future e-security risks mitigation initiatives

International co-operation among law enforcement agencies is key to mitigating e-security risks, since criminals now have global reach that's multiplied through use of global botnets.

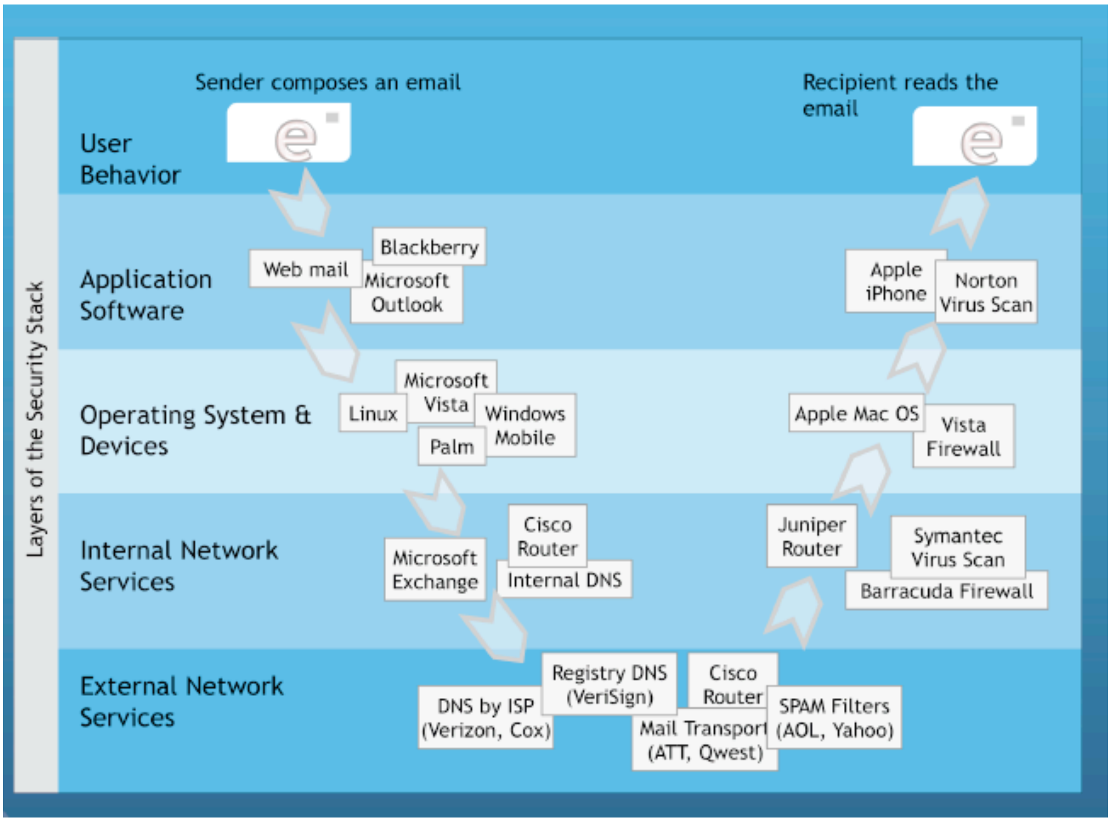
In the next year, the internet will experience an enormous growth in top-level domains (TLDs). ICANN, the Internet Corporation for Assigned Names and Numbers, plans a wide-open process to allow new TLDs in the domain space. Under this proposal, anyone could apply for any string as a TLD. If their application makes it through ICANN's objection and contention process, the applicant could then sell second level domains within their top-level domain. For example, an environmental group could apply for a TLD such as *.eco* and sell second level domains to organisations and businesses (*airbus.eco*, *ford.eco*, *hotels.eco*, etc.).

The new TLDs will exponentially increase the possible sources of cyber crime and attacks. We are encouraging ICANN to improve security requirements and contract enforcement tools so these new TLDs don't create new threats.

ICANN is also looking to enable non-Latin versions of TLDs known as Internationalised Domain Names (IDNs). The introduction of IDNs will allow billions of new Internet users get online using their native languages. These new IDN users, however, will not be aware of the tricks and techniques used in phishing and online fraud. These new users won't likely have anti-virus protection and not yet aware of the risks of downloading files or attachments, so they could easily become victims of e-crime. Moreover, their computers could easily become new nodes in bot networks. For the benefit of all, it is critical that education campaigns are targeted at these new users, using their own language and scripts.

f) Emerging technologies to combat risks

Fortunately there is a range of technologies deployed up and down the security stack to combat e-security risks. The diagram below shows security technologies involved when an email moves from sender to recipient.



More effective security will require continual vigilance whilst strengthening all the elements of the security stack. With our interest in e-commerce, NetChoice is particularly concerned with solutions that make the payment process safer and more trusted by the consumer.

At the moment, credit cards are the dominant method to pay for goods and services online. Credit card transactions are usually undertaken without any additional verification such as a PIN or password. Clearly, for most e-commerce users, this is not a problem. Consumers trust they are dealing with a reputable merchant and believe that their credit card company will cover them for fraud losses.

But securing a credit card facility can be a daunting challenge for small businesses or merchants just dipping their toe in the water of e-commerce. They often fall back on bank transfers as their default payment method for online transactions.

However, NetChoice argues that potential online shoppers are put off by the lack of verification measures on credit card transactions, or the potential risk that their credit card details could end up in the hands of fraudsters. Direct bank transfers also have their weaknesses: users may mis-key the account details of the merchant, and there is little or no protection offered by banks when things go wrong.

There are a number of other, internet-specific payment methods that address these concerns, such as PayPal, Paymate and POLi. These payment methods do not convey bank account or credit card numbers to the merchant, virtually eliminating the risk of identity theft or account fraud.

NetChoice believes the uptake of ‘safer payments’ measures depends on online merchants and marketplaces seeing a competitive advantage in being a safer payment provider. But there is a danger that this shift to safer payment methods could be undermined by regulatory. Rather than raising standards, premature regulatory intervention could slow uptake of safer payments and ultimately impair efforts to increase digital confidence.

As noted above, the Internet will soon add its second billion users, many of whom will be able to use their native language scripts in domain names and email addresses. These new users must be educated about safe online conduct, including encouragement to use payment methods that reduce risks of identity theft and unauthorized charges.   NetChoice and other security experts made recommendations to this effect at the ICANN meeting in Sydney on 25-June this year.

Conclusion

The two most effective means for government to address e-crime are stronger law enforcement and more education for business and users. NetChoice supports efforts along these lines.

However, NetChoice does caution the Committee against measures that while well-meaning, create additional regulatory burden for the e-commerce community. E-commerce is a young, dynamic industry. But it is characterised by small companies who are poorly placed to absorb the deadweight cost of unnecessary regulations.

Please feel free to contact me if you have any further questions.

Yours faithfully,

Steve DelBianco
Executive Director
NetChoice