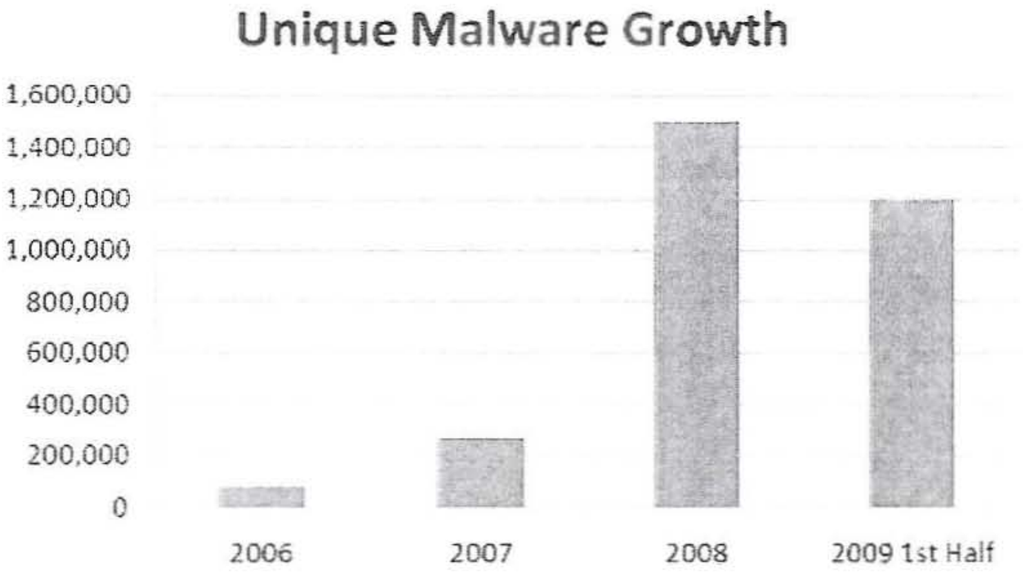
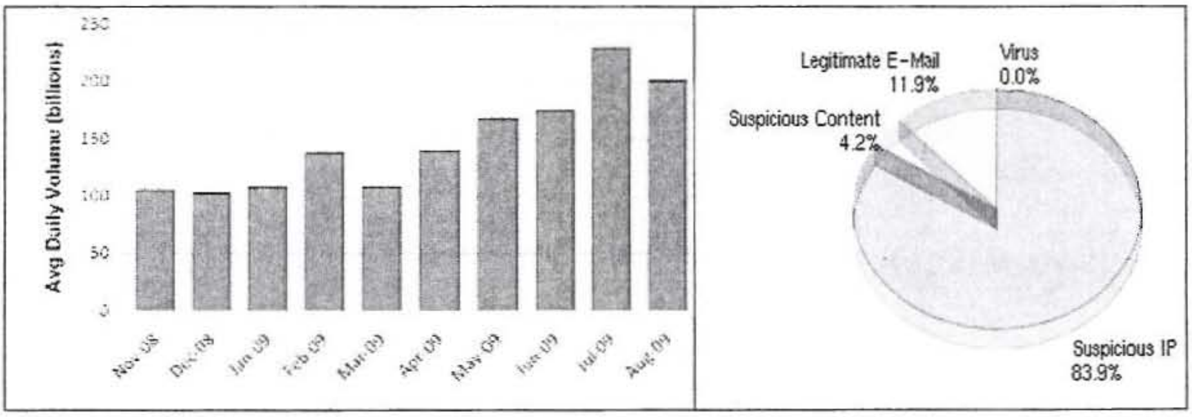
SUPPLEMENTARY SUBMISSION NO. 43.1

House of Representatives Committee on Cyber Crime

1. **Can Telstra provide statistics showing the extent of cybercrime?**



Source: McAfee Avert Labs (2009)



SPAM Statistics
Source: Cisco Systems, Inc

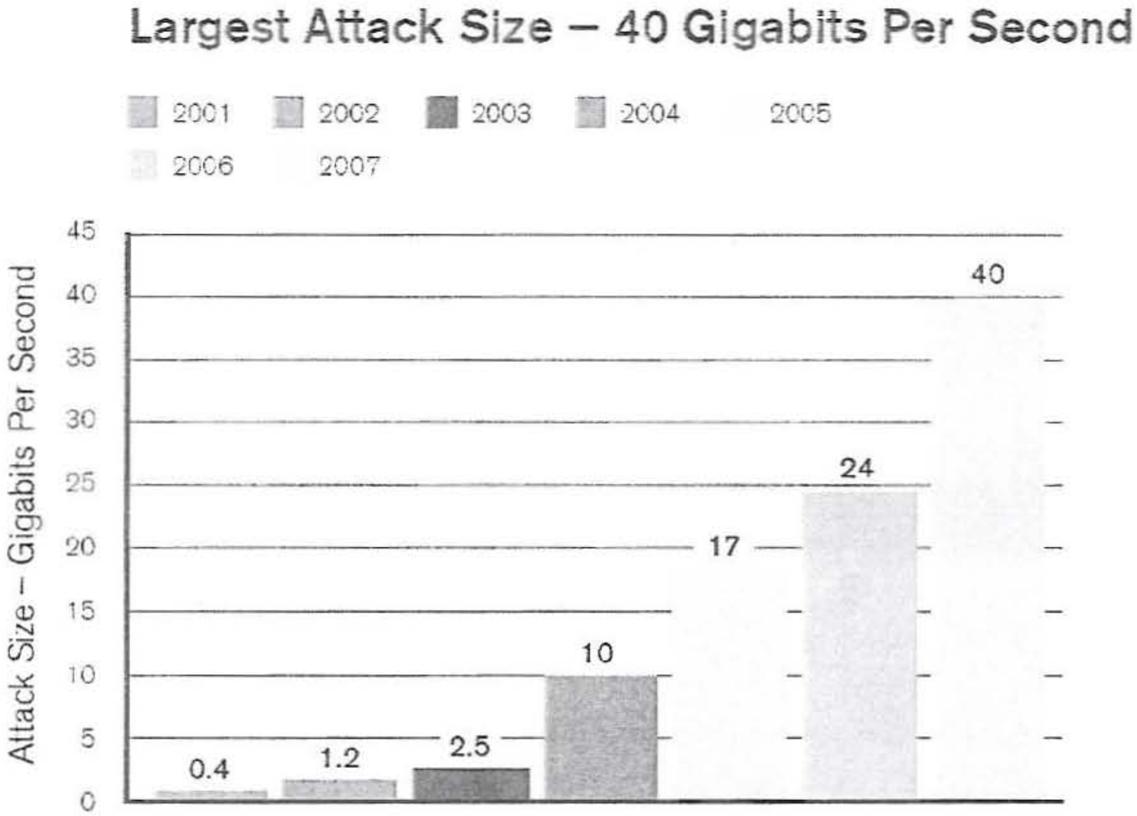


Figure 1: Largest Attack Size – 40 Gigabits Per Second

Source: Arbor Networks, Inc.

2. Is it feasible to require that home routers prompt the customer to change the factory password at the time of initial installation? If so, are there any downsides?

- Telstra has secured BigPond home wireless gateway/router products (initially via our installation CD and currently at the factory) since they were first introduced in 2004.
- Today all of our wireless gateways are secured with a unique security key (both a SSID code and a Wi-Fi pin which is ten digits long). This key offers Wi-Fi Protected Access (WPA) and WPA2-grade protection. The unique security key is applied at the factory meaning consumers are protected from the moment they set up their home network.
- This also means Telstra eliminates the potential of weak passphrase choices by automatically generating and distributing strong keys.
- While Telstra isn't in a position to comment conclusively on what other vendors do, we do understand that many 3rd party devices do not have this protection set up by default.
- This combination of SSID code and pin code is very difficult to break.
- We believe it would be unlikely that consumers would need to change these passwords once they are established – unless codes are compromised by persons with access to the unique key information bundled with the device.
- It is possible to change device security keys if required. The downside is that password information on all devices connected to the wireless

gateway (notebooks, PCs, games consoles, media players etc) also has to be manually updated with new password information.

- With more and more consumers connecting more and more devices to their Wi-Fi networks there is a balancing point between ensuring optimal security and accessibility. Telstra believes its Wi-Fi security implementation achieves this balance.

3. Does Telstra have any comments on the (Identity Crimes and Other Measures) Bill 2008?

Identity crime has the potential to cause harm to both industry and consumers and, as such, Telstra supports the Commonwealth's attempt to tackle identity crime; particularly where personal information is misused in order to commit such crimes.

4. Can Telstra provide a list of Cyber safety grant recipients and the amounts allocated from the Telstra Foundation since the "spotlight on Cybersafety" was announced?

In February 2008, the Telstra Foundation committed to putting a 'spotlight' on Cyber Safety. Our goal is to build the protective factors for children and young people to help them develop the skills needed to enjoy the use of information and communication technologies in safe, supported environments. This commitment was reaffirmed in April 2009 and annually $1m is allocated to projects in this program.

- $6 million over six years is committed to this focus area (commitment ending 2012/2013)
- Currently there are eight projects being funded:

i. SuperClubsPLUS Australia (La Trobe University) – a protected online learning community for Australian primary school children. SCPA has received funding of $1,542,514 over three years.

ii. Loddon Mallee Cyber Safety, CentaCare Sandhurst - Focusing on the need for relevant rural research around young peoples' behaviours, attitudes, risks, harms and protective functions, $270,000 committed over three years towards this project.

iii. Parent education program and resources, Edith Cowan University - $341,000 committed over three years.

iv. Smart Online Safe Offline (SOSO), NAPCAN - $534,000 committed over three years to support the development of a digital communications strategy to educate young people how to stay safe within their online environment.

v. A youth led public debate on cyber safety, Student Youth Network- $80,000 committed over two years to this project as the sole funder.

vi. A cyber smart campaign to create cultural change in cyber space, The Alannah & Madeline Foundation - $200,000 committed towards the project.

vii. Berry Street's BeNetWise - $206,000 committed over one year to assist vulnerable children in out of home care, who have not had access to the internet, to develop skills and protective behaviours to access and use technology safely.

viii. The Inspire Foundation, Technology and Wellbeing Roundtable - a grant of $145,000 over one year to support the advancement of the Technology and Wellbeing Roundtable, an alliance of government, corporate and not for profit organisations that view technology as an enabler of young people.

5. Does Telstra have a view on whether the voluntary E-Security Code should be mandatory? If we do not support it being a mandatory code, why?

Telstra is supportive of the E-Security Code continuing to be voluntary. Self regulation typically promotes good practice within the industry, has lower compliance costs on businesses, and also allows both large and small industry participants to respond more quickly and efficiently to issues, especially in an area such as this where the environment is dynamic and new issues are emerging continually. The main aims of the voluntary e-security Code are to:-

- Encourage ISPs to actively check for suspicious activity within their networks and source information on compromised computers, through participation in the Australian Communications and Media Authority's Australian Internet Security Initiative or by seeking information from other sources.
- Encourage ISPs to report repeated or severe instances of suspicious activity to relevant Government agencies, where it is believed the suspicious activity constitutes a serious threat to Australian communications networks[1]: and
- Provide both industry and customers with a resource that can be trusted to provide the information they need to understand and resolve an e-security issue.

We support a voluntary code that will assist and encourage all ISPs to follow certain recommendations on the identification and reporting of potentially compromised customer computers that are a security threat not only to Australian customers but also to the integrity of the Internet. Some e-security risks can be responded to by ISPs using standardised solutions very quickly but there are other more sinister e-security risks (such as the Conficker Worm[2]) that require ISPs to act cooperatively on a voluntary basis to resolve with Government.

6. Where does liability sit when a customer has been impacted by cybercrime? With the ISP or someone else?

It is not possible to determine where liability sits for cybercrime, as it will depend on the individual cybercrime activity. These include but are not limited to who was responsible for the item/device/thing that allowed the unauthorised access, what actually happened, was it reasonably foreseeable that it could happen, had there been warnings about it happening, what security measures were in place, etc.

[1] Draft Internet Service Providers Voluntary Code of Practice for Industry Self Regulation in the Area of e-Security, version 1.7

[2] http://www.smh.com.au/technology/security/internet-meltdown-threat-conficker-worm-refuses-to-turn-20090922-fzlh.html