SUBMISSION NO. 28

RSA®

The Security Division of EMC

House of Representatives Standing Committee on Communications New Inquiry into Cyber Crime

A submission from RSA, The Security Division of EMC

Table of Contents

Introduction

Significant challenges lie ahead for governments, law enforcement organisations and the online security industry to protect Australian consumers during the coming years.

The nature of threats is steadily growing and groups behind online fraud are multiplying.

RSA believes this scenario requires increased diligence on the part of consumers, greater educational efforts from government and the industry and legislative change to provide a greater level of protection.

Key Recommendations

The recommendations contained in this paper have been designed to assist the House of Representatives Communications Committee during its review of e-security. RSA welcomes the opportunity to provide additional information in support of this paper or engage in further discussion with the Committee.

RSA's key recommendations can be summarised as follows:

- Drive both Federal and State Government to update legislation to adequately deal with cyber crime;
- Legislate mandatory disclosure and reporting of data breaches;
- Allocate funding and resources at Government level to address the issue of cyber crime; and
- To facilitate all Government agencies to have standardised methods to detect and respond to cyber fraud and cyber criminal activity.

Contact

Please contact Mark Pullen, Country Manager of RSA Australia and New Zealand, on:
Phone: (02) 8912 6177
Email: mark.pullen@rsa.com
Address: Level 6, 60 Miller St,
North Sydney, NSW 2060

About RSA

RSA, the security division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organisations succeed by solving their most complex and sensitive security challenges. RSA's approach to security guards the integrity and confidentiality of information throughout its lifecycle - no matter where it moves, who accesses it or how it is used.

Headquartered in the United States, RSA has a considerable presence in Australia and provides security solutions for many of the leading enterprises and government organisations based in this country.

The current cost and level of threat to consumers

The Australian Bureau of Statistics estimated in 2008 that consumer fraud – both online and other forms – was costing consumers a combined loss of almost 1 billion dollars.

According to the study, Personal Fraud, June 2008, a total of 806,000 Australians aged over the age of 15 were victims of at least one incident of personal fraud.

The RSA Anti-Fraud Command Centre, which monitors illegal online activity in more than 140 countries, has found that Australia consistently rates amongst the 10 top most attacked countries – in terms of total number of attacks and number of businesses, or brands, targeted. According to the Centre this is comparable to the number of threats in countries such as Canada, South Africa and India.

For its part the RSA Anti-Fraud Command Centre has shut down more than 150,000 phishing attacks and reduced the average shutdown time of attacks from 115 hours to five hours. During the past 12 months it has seen the monthly number of phishing attacks stabilise – observing between 10,000 and 15,000 attacks per month.

Understandably this level of attack has kept consumer concern very high, although preventative action is still quite low.

A study released in March 2009 by the Australian Communications and Media Authority showed 61 per cent of Internet users and 64 per cent of non-Internet users were concerned about potential identity theft because of technology changes.

However, 51 per cent of Internet users in the study had not undertaken even preliminary security measures – such as installing anti-virus software on their home computer.

For those who do take precautions there is still a threat that their personal information – from credit card information to driver's license details – could be compromised by a third party. More worryingly is that they may not know their details have been misplaced or stolen for some time.

Under current Federal legislation businesses are not required to notify individuals when their personal information has been compromised.

The Australian Law Reform Commission handed down its report into the Privacy Act in May 2008 which recommended the introduction of mandatory reporting when a data breach had occurred. The report suggested a balance needed to be struck between harm to individuals and the cost of prescriptive notification measures.

So far no legislative developments have taken place.

Developing threats

RSA has detected a number of changes in the technology and approach by online criminals that will prove challenging to safeguard consumers against.

From a technology perspective, the rise of fast-flux Botnets has the potential to cause increasing headaches for the security community. Fast-Flux is a technique that uses a network of compromised computers, known as a botnet, as a conduit between the content server and its targets.

In 2008, 44 per cent of phishing attacks detected by the Anti-Fraud Command Centre were hosted on a fast-flux network and RSA expects to see this number steadily increase in the near future – moving past the adopter stage and becoming a mainstream hosting method by online criminals .

Shutting down these types of attacks is complex, as the originator of the attack is hidden behind a cloud of compromised machines – causing a constant rotation of IP addresses and thus avoiding detection. As an example, an attack on a bank in Australia could originate in Estonia via a network of compromised computers in Mexico.

For Australian consumers this means long-lasting attacks that persist well after initial consumer alerts have been issued. Online users will be asked to be constantly vigilant for specific types of attacks rather than just bracing for a shorter period.

The second impact for Australian consumers is related to the scalability of fast-flux networks. They are both easy to set up and quick to deploy. Service providers in the fraud community now rent the entire necessary infrastructure to other criminals.

In fact, Fraud-as-a-Service is likely to grow, with everything from telephone call centres, customised Trojan infection services and HTML injection kits available as a subscription service or for a flat fee.

The implication is that technical know-how or technology investment is no longer a prerequisite for criminals interested in participating in online crime. For Australia this means the possibility of more attacks on local consumers, as well as the potential for more people from Australia being involved in the attacks.

Australia was responsible for hosting 3 per cent of the world's phishing attacks in April 2009, more than those originating in countries such as Russia and only slightly behind the United Kingdom and Canada.

A cohesive approach

There are many resources from which Australian consumers and businesses concerned about security can draw. The Government's Stay Smart Online website alone lists 50 additional Australian resources for reference.

However, the coordination of these resources is unknown to RSA. Individually they provide valuable information for consumers – particularly those like Stay Smart Online and SCAMwatch.

At the request of Australia's banks for the better good of consumers, RSA is working closely with the Australian High Tech Crime Centre (AHTCC) to shut down criminal activity such as phishing attacks. The AHTCC is charged with combating serious and complex high tech crimes, especially those beyond the capability of a single jurisdiction.

Private industry associations and their security solution-providing members, however, cannot gain the upper hand on their own. Due to its size and complexity, cyber crime is a major issue which is seeing the security industry move beyond educating people to protecting them. Added to this is the lack of funding, and need for online security policies and procedures. Governments must take a leading role in this area and must do so in a coordinated way.

Thus, while private companies, informed individuals and state and local government authorities should be invited to contribute ideas and resources as appropriate, it must fall to the Commonwealth to drive a single centralised effort to legislate internet behaviour in Australia.

The industry is well placed to contribute to such a single centralised initiative. Australian technology companies and individuals are amongst the most talented anywhere and companies such as RSA, moreover, are able to call upon a wealth of experience from both their product research and development operations and their worldwide customer security businesses.

Closing the information loop

In addition to protecting consumers, steps must be taken to safeguard their information when held by third parties.

As mentioned above, the Law Reform Commission has provided legislative recommendations that, if adopted, would compel third parties to notify customers or members if their personal data has been compromised.

Similar legislation already exists in countries such as the United States (such as California's privacy laws), and Australia would be well advised to follow this lead.

In addition to alerting consumers to potential loss, such legislation would also provide businesses with a degree of certainty around their responsibilities and the protection of consumer data.

Businesses are increasingly vulnerable to potentially serious economic, legal and social repercussions simply because they don't know what is required of them with regard to data breach notification.

RSA is asking the Government to provide legislation that provides businesses with greater clarity into their responsibilities, while at the same time protecting the private information of individuals.

Conclusion

Australia comes from a reasonably strong platform of providing consumers with information and technology to protect themselves online.

The next 12-18 months will invariably prove challenging, in this country as it will in others. However the extension of educational efforts, funding, greater coordination and the introduction of prudent legislation and mandatory reporting are required to provide a layer of ongoing protection.

RSA thanks the House of Representatives Communications Committee for allowing this submission and welcomes further discussion on this very important topic.

---ooo0ooo---