SUBMISSION	PARLIAMENTARY COMMITTEE	27 AUGUST 2009	UNCLASSIFIED - PUBLIC
FORMAT	AUDIENCE	DATE	CLASSIFICATION

Australian Government
Australian Taxation Office

Australian Taxation Office

Response to the House of Representatives Standing Committee on Communications

Inquiry into Cyber Crime

UNCLASSIFIED - PUBLIC

TABLE OF CONTENTS

INTRODUCTION

The material in this document is provided by the Australian Taxation Office (Tax Office) in response to the House of Representatives Standing Committee on Communications – Inquiry into Cyber Crime. Information has been provided in categories using the terms of reference of the Inquiry.

BACKGROUND

The Tax Office has been providing online services to its client segments since the introduction of the Electronic Lodgement System (ELS) in 1989. This system was provided for use by tax agents initially to lodge income tax returns on behalf of their clients and has expanded since then to offer many other online services. In 1997, the e-tax system was first introduced to allow Australian citizens to lodge their income tax returns online. Currently over 2 million returns are received through e-tax.

Since the introduction of A New Tax System in 2000, the Tax Office has introduced many more online services in the shape of portals for tax agents and businesses, stand alone software tools such as e-Record and the Electronic Commerce Interface (ECI) which provides for online submission of Activity Statements, PAYG summaries, Excise claims, TFN declarations, Superannuation contribution statements and other reports.

The Tax Office currently interacts online with a very wide range of the citizen and business community, from students, parents and pensioners, through to micro, small and medium to large businesses.

Currently, the Tax Office is playing a key role in the development of the Standard Business Reporting (SBR) initiative and will be progressively delivering a number of services through this new online channel.

Over the course of time that the Tax Office has been delivering online services, the Tax Office has developed numerous policies and capabilities to deliver secure online services to the Australian community and to drive increasing community take up of the services provided. This document provides some general observations that draw on Tax Office experience and also provides details that reflect the current eSecurity activity and direction.

GENERAL COMMENTS

The following general comments on cyber crime are provided from the perspective of the Tax Office.

1. As a large government agency providing many online services to the Australian community, the Tax Office is continually seeking to balance the ease of access to and use of online services, with the level of security that it requires to enable the community to interact safely.

2. The greatest cyber crime vulnerability that the Tax Office faces is loss of revenue or information through identity fraud. This of course has major impacts on the Australian community as well. In addition to the harm caused to the person whose identity is stolen, it can lead to a loss of confidence in the tax system which has major ramifications for the Australian community.

3. There are many different eSecurity approaches (processes and technology) employed by government agencies delivering online services to prevent cyber crime but the approaches are varied and this may provide a greater number of opportunities for cyber crime attacks. At the same time, different approaches to online service delivery by agencies makes it difficult for a consumer (who is common to these agencies) to create an easy and safe operating environment when interacting online. The Tax Office plans to transition its business clients from its current ATO credential system to the new ABR credential system being developed to support the Standard Business Reporting (SBR) initiative. Businesses will have one simple means to interact online – not only with the Tax Office but other Federal and State agencies. This multi agency approach to provide access for businesses to online services will provide secure solutions that are simple and consistent for users. A multi agency or whole of government approach to authentication will also realise cost savings for all parties. At this point the Tax Office is not aware of an equivalent solution for citizens.

The Tax Office has been operating in an online service delivery environment for about 20 years and has developed numerous strategies and capabilities over that time in regard to managing the issue of cyber crime. In addressing the terms of reference in written form it is difficult to know whether the value that the Tax Office can provide to the Inquiry has been fully realised. Consequently, the Office would welcome the opportunity to present oral evidence to the Inquiry members.

SUBMISSION DETAIL

TERMS OF REFERENCE

a) Nature and prevalence of e-security risks including financial fraud and theft of personal information … including the impact of malicious software such as viruses and Trojans;

The Tax Office has identified a 31% increase in IT security incidents impacting on Tax Office systems in the 2008 / 2009 financial year compared to the previous financial year[1]. Such incidents included attempts to phish for information as well as malware attacks.

More recently there have been a number of tax refund email (phishing) scams. The emails used to catch the consumer are visually very convincing. In addition to the personal loss or risk to the consumer associated with these attacks, they pose a risk of loss of information or revenue from the Tax Office through identity fraud. Recent phishing examples are as follows:

- Victims were lured by email to a bogus website which was a mirror image of the Tax Office website, hosted on an international server (identified in the Ukraine). The email offered a substantial tax refund ($9,500). This particular site was primarily designed to harvest personal information, passwords, credit card information etc.
- The use of voice over the internet protocol (VoIP) technology in recent a 'cold-calling' approach by scammers in Australia saw potential victims directed to phone the VoIP number and provide their personal information;
- Scammers contacted taxpayers via mobile SMS text messaging requesting them to send similar details as in phishing emails;
- With the announcement earlier this year of the tax bonus payment to current taxpayers, phishing and other scam variants were deployed rapidly by criminals to target individuals susceptible to these methodologies, which were again an attempt to harvest credit card details and other personal data;
- Also, with the new tax year about to begin, during one week alone in June this year, 8 variations of a tax refund scam similar to above have been identified. The primary intention of these scams is the harvesting of personal banking information to obtain funds from bank accounts and credit cards.

The use of the internet by taxpayers as a method of transacting with the Tax Office is continuing to grow. For example during the 2007-08 financial year more than 90% of income tax returns were lodged electronically. Tax Office operational activities have identified that the overwhelming majority of current refund fraud cases (often enabled by identity crime) are facilitated through internet lodgement.

[1] Information provided by ATO ICT Trusted Access – Vulnerability Management and Research.

Since 1 July 2008 the Tax Office has finalised 35 prosecutions (23 GST, 11 Income Tax and 1 Excise) where refund fraud was the primary risk element. Results of these prosecutions included:

- 29 custodial sentences
- 5 good behaviour bonds
- 1 community service order
- $1.5 million in reparation orders

In respect to identity theft issues, there is minimal evidence to suggest that the point of compromise has been unauthorised external access to Tax Office information technology systems. However, the use of malware by criminals operating within Australia and overseas has been steadily growing in use, primarily targeting the banking and financial sectors but as these sectors address vulnerabilities, other sectors such as the government may become more popular targets.

In the context of combating cyber crime, some more technically oriented areas of research in the Tax Office include:

- effective and secure management of a mobile working platform for an organisation the size and distribution of the Tax Office (e.g. laptops, mobile phones, PDA devices etc)
- management of new and emerging technology with higher levels of function integration within the one device, providing new and possibly broader avenues for cyber crime
- the increasing sophistication of aggregated, non-destructive, cyber crime attacks, where the main purpose is information gathering i.e. identity credentials, accounts and financial details
- the increased presence of malcode invading not just websites, but forums, blogs and even search engines
- the increasing use of VoIP as a phishing exploit
- the increasing prevalence of social networks such as Face Book and My Space which may lead to increased identity fraud attacks on Tax Office online services
- paradigm shifts in the way IT is used, such as cloud computing and virtualisation software where new opportunities for cyber crime might occur
- loss of data outwards from the Tax Office through various channels such as email
- botnets and their availability for hire in order to commit cyber crime

The Tax Office has a significant investment in IT staff whose role is closely related to research into and the detection, the follow-up and the prevention of cyber crime.

b) The implications of these risks on the wider economy, including the growing economic and security impact of botnets;

Many cyber scams are primarily intended for the harvesting of personal banking information, used to drain victim's funds from bank accounts and credit cards. Once this data is obtained it can however provide additional opportunities for criminal syndicates to attack government agencies and the banking and finance sector in other ways.

The use of the tax system to gather information for financial gain and to support other forms of crime has a potentially significant impact on the integrity of tax administration and the reputation of the Tax Office. In addition to targeting Federal monies through fraudulent Tax Office refunds, criminal syndicates would value highly the large volume of taxpayer information which is held by the Tax Office which could be used for a range of illicit purposes.

c) Level of understanding and awareness of e-security risks within the Australian community;

The Federal government has introduced a number of initiatives to assist the public and business to have an understanding and awareness of eSecurity risks. These include websites such as Stay Smart on Line, SCAMwatch (maintained by the ACCC) and FIDO (maintained by ASIC).

The Federal government also sponsored the recent National E-security Awareness Week held 5 – 12 June 2009 which included a conference in Sydney facilitated by the Australian High Tech Crime Centre, University of Technology Sydney and Australian Institute of Criminology (AIC). The conference was attended by a wide range of representatives from law enforcement, government (including the Tax Office), the legal profession and judiciary, academia and private industry participants. This conference was highly valuable in terms of raising the awareness of key stakeholders in existing and emerging cyber crime risks.

The Tax Office has issued a number of media releases in regard to phishing attacks that have been circulated under the guise of Tax Office refunds or stimulus payments, which were in reality attempts to harvest the credit card details of victims. Similarly the Tax Office displays prominent warnings on its internet home page in respect to cyber crime threats (particularly phishing emails), as well as general on line security advice.[2]

Anecdotal information gathered by Tax Office shopfront staff is to the effect that some tax payers from a non English speaking background appear to have a limited understanding and awareness of eSecurity risks. Their limited knowledge and understanding of the Australian taxation system, lack of English language skills and for some, general computing inexperience, leave this section of population potentially vulnerable to online exploitation.

The Tax Office does not have a current mechanism for measuring the understanding and awareness of eSecurity risks within the broader Australian community. With the increasing threat of cyber crime this could potentially be an area appropriate for research; and could allow this organisation to compile a broader base of research - building upon the knowledge gained through the Australian Business Awareness study.

Surveys of Tax Office clients in relation to interactions with the Office, while showing an increase in awareness of security issues associated with dealing online, show that clients still take risks online either because they are not aware of the potential impact on them or they take a risk for expediency's sake.

[2] Australian Taxation Office, *Online Security*, available at internet at http://www.ato.gov.au/onlineservices/content.asp?doc=/content/62347.htm&page=2&H2

d) Measures currently deployed to mitigate e-security risks faced by Australian consumers

i) Education initiatives

The Tax Office contributes broadly to raising awareness of cyber crime within the community and with key stakeholders. In addition to advice that is available on the Tax Office website, communication strategies have included media releases, which inform the community of the safe way to interact with the Tax Office and which provide alerts to the means by which fraud syndicates attempt to obtain taxpayers personal information for illegal use.

An educational awareness program, focussed on identity fraud within particular non English speaking background groups, has resulted in a number of articles being published in local community based newspapers. Tax Office shopfront and call centre staff received nationwide identity crime training in 2006, which has since been adopted as part of a staff induction package at call centres.

The Tax Office also has a program to systematically provide advice to tax agents to ensure the safeguard of their client information. This has been provided through online advice available on the ATO website and through various publications, including the TAXAGENT magazine and Seminar Guides. The Tax Office has also introduced more secure mechanisms (digital certificates) for tax agents to conduct on line transactions with the Tax Office.

Specific examples of community oriented education initiatives include:

Web alias – **www.ato.gov.au/identitycrime**

- Information advising taxpayers to keep their TFN safe and not provide TFN / identity details on online job ads, etc

'Keep your TFN safe' postcards

- Available in English and 12 foreign languages

Security, Fraud and Prevention discussion

- Relationship Managers talk with Tax Agents about the key messages including strategies to protect their clients from falling victim to identity theft

ATO Tax Practitioner Forum

- Briefings by the Tax Office on identity crime and refund fraud and other eSecurity issues

Business Activity Statement service provider newsletter

- A monthly subscription email newsletter, which aims to engage and educate bookkeepers

Key Message Guide

- The Key Message Guide is a summary of messages for media spokespeople and communication practitioners delivering Tax Time campaign activities.

Activity Statement Update

- The ASU goes out to:
  - over 2.8 million activity statement preparers each quarter
  - 150, 000 who lodge electronically using the portal will receive the newsletter via email, and
  - It is also available as a html on ato.gov.au and is read by tax agents and industry groups

E-link

- Online communication to tax agents

NewsExtra

- Tax Office staff internal communication

Tax Time media fact sheets (also in foreign languages)

- Articles on schemes, scams and identity fraud and keeping your TFN safe

Google Ad Words

- Banner Ads on TFN protection and identity theft appear on websites when people search terms relevant to foreign workers, identity protection and international students

TFN Advice Letter (Individual, Non-individual, Non-resident)

- Updated the letters to include information to taxpayers about keeping their TFN safe

Student VIP email

- Email distributed to 180,000 students (20,000 international students) about protecting their TFN to avoid identity crime
- 400,000 banner ads on the Student Services Australia website about TFN protection

Tax Evasion Avoidance and Crime e-magazine article

- Identity crime article will appear in the first e-magazine

Shopfront identity crime awareness package and ‘Keep your TFN safe’ quick reference guide

- Training packages for Shopfront staff to help them understand identity crime and distribute the postcards

Identity Crime and Refund Fraud mitigations strategy

- Communications strategy prepared for Tax Time 2009 to mitigate the risks associated with identity crime and refund fraud

Long term communication strategy

- Will tie in with the Attorney General’s National Identity Security Strategy and those of other external agencies

Online services presentations

- Presentations conducted internally on an annual basis to staff that include information on how clients can protect themselves online and ensure their digital security

SBS radio scripts

- TFN security for emerging language groups, Indigenous groups and for the Print Handicapped

Online security page

- Includes information on current and planned activities involving email and SMS, how to ensure your online security, the latest Tax Office related scams, and examples of scams

ii) Legislative and regulatory initiatives

In support of the SBR initiative, changes to the Australian Business Number legislation (Amendment (2009 Measures No.2) Bill 2009: Australian Business Register) have been made to allow the Australian Business Registrar to register and issue online authentication credentials. These are to be used by Australian businesses to interact with government bodies across the three tiers of government in Australia. Key amendments are to:

- tighten the security around this process with amendments to the existing Australian Business Number Act were sought - Tax Laws Amendment (2009 Measures No.2) Bill 2009: Australian Business Register
- include an additional condition to be satisfied before the Registrar must register an entity in the Australian Business Register. The additional condition provides the Registrar with the authority to request information or specified documents that the Registrar needs to be satisfied that the identity of the listed associates is established.
- allow for the Registrar to register and maintain details about representatives of businesses to enable electronic communication with one or more government agencies. The amendments allow the Registrar to identify representatives of businesses as part of the registration process. The amendments also require the entity or the representative to update the details on the Register. The Registrar is able to use public information and information provided by third parties on a voluntary basis to update and correct the Register in respect of details of representatives. These amendments have been passed and will come into effect on a date to be proclaimed.

There are specific offences found in the Commonwealth Criminal Code Act 1995, Part 10.7, which cover computer related offences, including hacking and destruction of data. Currently there are no specific offences related to identity crime. However, it is believed that this legislative deficiency will be rectified in the Model Criminal Code[3].

[3] This will be a revamp of the Commonwealth Criminal Code Act 1995.

iii) Cross-portfolio and inter-jurisdictional coordination

To provide secure access to online systems for Australian businesses, the Tax Office currently operates a digital certificate system for Australian business staff so that they can interact with the Tax Office on behalf of the business. The registering and issuing of digital certificates involves a proof of identity of the person holding the digital certificate and also a proof of their association with the business. The ongoing operation of this system requires a large investment of people and IT resources by the Tax Office.

The Tax Office is currently involved in numerous cross portfolio or jurisdictional initiatives that are leading to the delivery of online services in a more secure manner for clients. Key initiatives are:

- Standard Business Reporting (SBR)

  For the delivery of online reporting services, the SBR Program is creating a whole of government credential (digital certificate) for employees of a business to use to interact with the three tiers of Australian government – Federal, State and Local. The identity basis of the digital certificate will be the Australian Business Number (ABN) and the issuing of the digital certificate will be under the control of the Australian Business Registrar to ensure the integrity of the process.

- Australian Government Online Service Point (AGOSP)

  While the Tax Office provides a shared secret based option to allow citizens to lodge their tax returns online it is also engaged with the Australian Government Online Service Point (AGOSP) project with intent to, in the future, link the Tax Office option with a broader use AGOSP citizen credential if the level of assurance provided by the AGOSP credential is appropriate.

The Tax Office also has a close working relationship with a number of agencies and non-government bodies to enable the sharing of expertise and relevant information to head off or mitigate the impact of, security incidents. These include:

- Australian Federal Police (AFP)
- Australian High Tech Crime Centre (AHTCC)
- Defence Signals Directorate (DSD)
- AusCERT

The Tax Office can respond to breaches of eSecurity by denying access to the Tax Office online services to compromised users. New digital certificates can also be issued following any breaches.

The national Document Verification Service, when in place, can be used by government agencies at the Federal, State and Territory levels as it will be a reliable means of verifying identity documents.

The Tax Office is involved in the National Identity Security Strategy through all its associated working groups.

iv) International co-operation

International co-operation is facilitated through the AFP or the AHTCC, particularly in order to gain assistance to close down illicit internet sites. Furthermore, the Tax Office can liaise with its foreign counterparts in identifying issues and strategies to combat e-security breaches. AusCERT / GovCERT can also liaise with its international contacts to progress investigation of breaches of Tax Office internet protocols.

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

A future initiative can include scenario planning for critical e-Security incidents impacting on the Tax Office and other government agencies. This could potentially develop more timely and effective liaison and sharing of information, and would practice having compromised internet sites shut down by AusCERT / GovCERT; as well as test the closing of portals to limit the effectiveness of Trojans / malware.

A broader analysis of public e-Security should be conducted, as this would build upon the research already undertaken in respect to private business and prove to be valuable to a wide range of stakeholders and allow appropriate policy and legislation to be considered.

The Tax Office continues to explore automated data matching opportunities between agencies, ideally Federal and State, to minimise the impact of identity fraud. There are significant issues to be considered in achieving this, particularly in regard to the secrecy and privacy provisions of the law. There are also important considerations around the accuracy, quality and security of data held by different agencies.

Due to the specialised technical nature of investigating the eCrime trail, the Tax Office has been looking at the work undertaken in the United States in relation to accreditation of specialists and laboratories in the computer forensics field.

f) Emerging technologies to combat these risks.

The Tax Office continues to improve on and develop new early warning indicators of fraud and uses these to conduct automated risk assessments as a means of maintaining integrity of client records and preventing revenue loss.

The Tax Office will continue to further its understanding of security features employed by other public and private sector organisations for on line transactions, including two factor authentication (such as randomly generated and non-static proof of identity questions), tokens and/ or biometric security features (such as voice recognition) - which have been recently introduced by Centrelink and some private sector businesses.

The Tax Office would welcome access to any emerging technology that would enable the confidential and reliable validation of foreign identity documents.

The Tax Office is part way through a large project (called Centralised Audit Logging) designed to enhance its ability to provide an end-to-end picture of access and change activity by externals and internals accessing its systems. This end-to-end picture will be used to discover patterns and trends in online access and to detect or even prevent specific fraud activity.