New Zealand
National Cyber Security Centre

2013 Incident Summary

National Cyber Security Centre – 2013 Incident Summary

Foreword

The incidents summarised in this report reinforce that cyber security is truly a global issue, and New Zealand organisations are just as vulnerable as organisations in any other part of the world.

The 2013 National Cyber Security Centre (NCSC) incident summary reflects incidents which have been detected by the targeted organisations, reported to us, and which we have assessed as significant.

International experience indicates that these reported incidents are likely to be the tip of the iceberg in terms of the level of actual threat activity currently occurring on New Zealand networks.

Sophisticated threat actors often use tools and techniques which are not readily picked up by commercially available products, or standard network security provision, and therefore can often go undetected.

This incident summary is provided as a general indicator of threat activity, to help raise awareness of cyber security as an issue for all New Zealand organisations, regardless of size and the nature of the enterprise.

Over the past 12 months, the Bureau, the NCSC and our partners in the National Cyber Policy Office (Department of the Prime Minister and Cabinet) and the Chief Government Information Office (Department of Internal Affairs) have increased efforts to engage with industry and government to raise awareness of cyber threats and to enhance the resilience of our networks and systems.

Ian Fletcher
Director
Government Communications Security Bureau

Overview

The New Zealand National Cyber Security Centre (NCSC) provides enhanced cyber security services to New Zealand Government and private sector organisations to assist them to defend against cyber-borne threats.

As part of its functions, the NCSC records cyber security incidents affecting government agencies, critical infrastructure operators and private sector organisations. Reports are provided by affected organisations, researchers, IT security partners as well as local and international partners. All reported incidents are treated in-confidence and are notified to the NCSC via the reporting form located on the NCSC website.

The statistical information presented in these reports is provided to raise awareness and general understanding of the nature of the cyber-threat landscape facing New Zealand organisations and individuals.

Reporting

In the year to 31 December 2013 the NCSC saw a continued increase in the number of incidents reported and recorded, from a total number of 134 recorded incidents in 2012, to a total of 219 in 2013.

We believe this increase can be attributed in part to greater awareness of the importance of reporting incidents among the New Zealand government agencies and critical infrastructure providers, and also awareness of the role and functions of NCSC.

Incidents must meet certain criteria designed to differentiate them from other common events, experienced in the on-line environment, before they are logged by NCSC personnel. A single incident could include multiple IP addresses, websites, networks and servers, organisations or affected parties.

Case studies

This Summary provides three case studies which have been drawn from actual incidents which were reported during 2012-2013. These provide context to the trends reported by the statistics, and also illustrate the impact that these incidents have on New Zealand organisations.

Incident Types

The graph 'Category Breakdown' (Fig 1.1) provides a breakdown of the incident reports as categorised by type.

Scam & spam related incidents were the largest category of reported incidents at 30%. Denial of service (DoS) attacks and Botnet/Malware activity were the second largest categories making up 22% and 12% of incidents respectively.

Other significant issues captured include network intrusions (7%), website compromises, hijacking & defacement (6%) and Spear Phishing (5%).

Fig 1.1

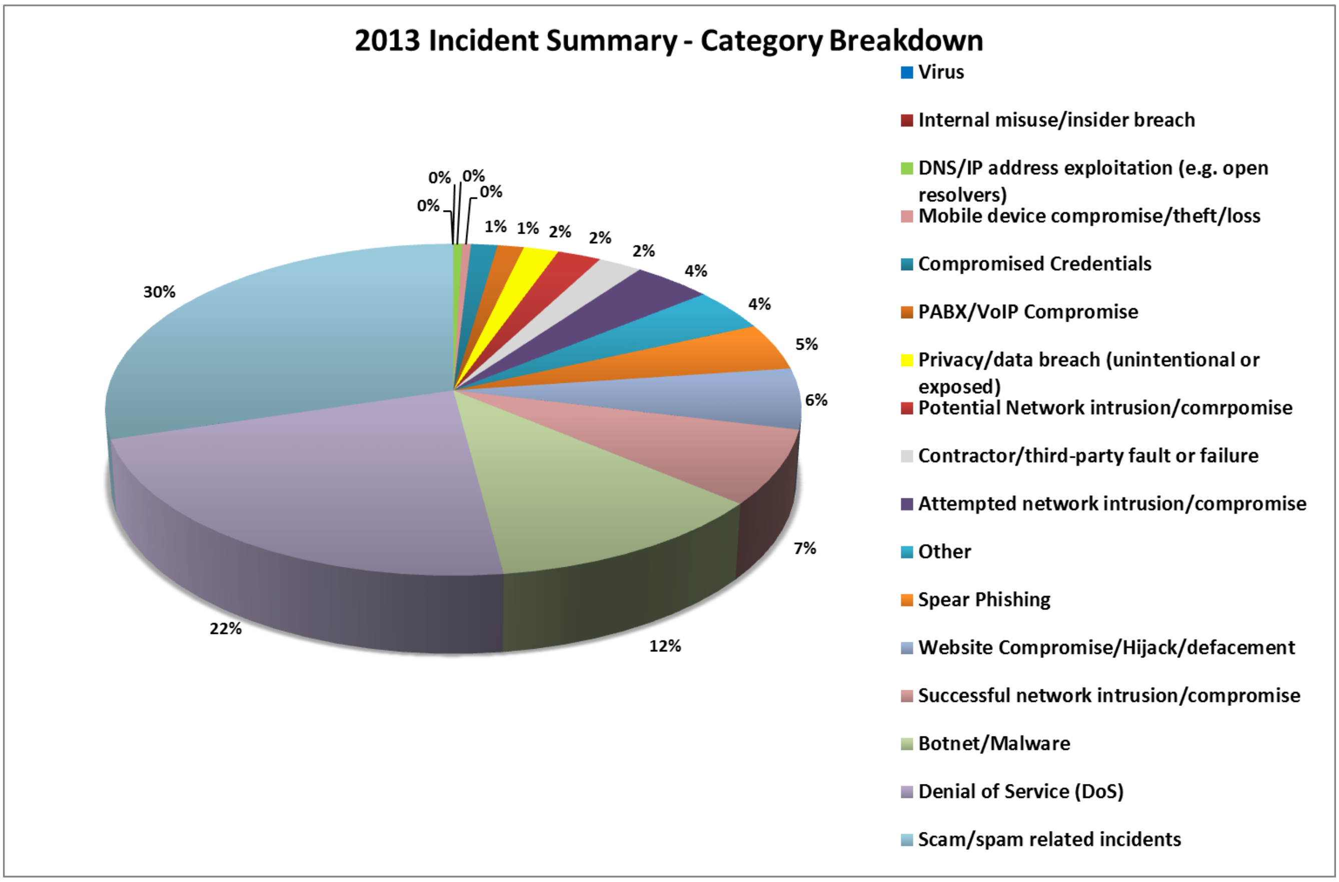


Figure 1.1 indicates New Zealand is broadly in line with international trends for the types of cyber incidents.

Fig 1.2

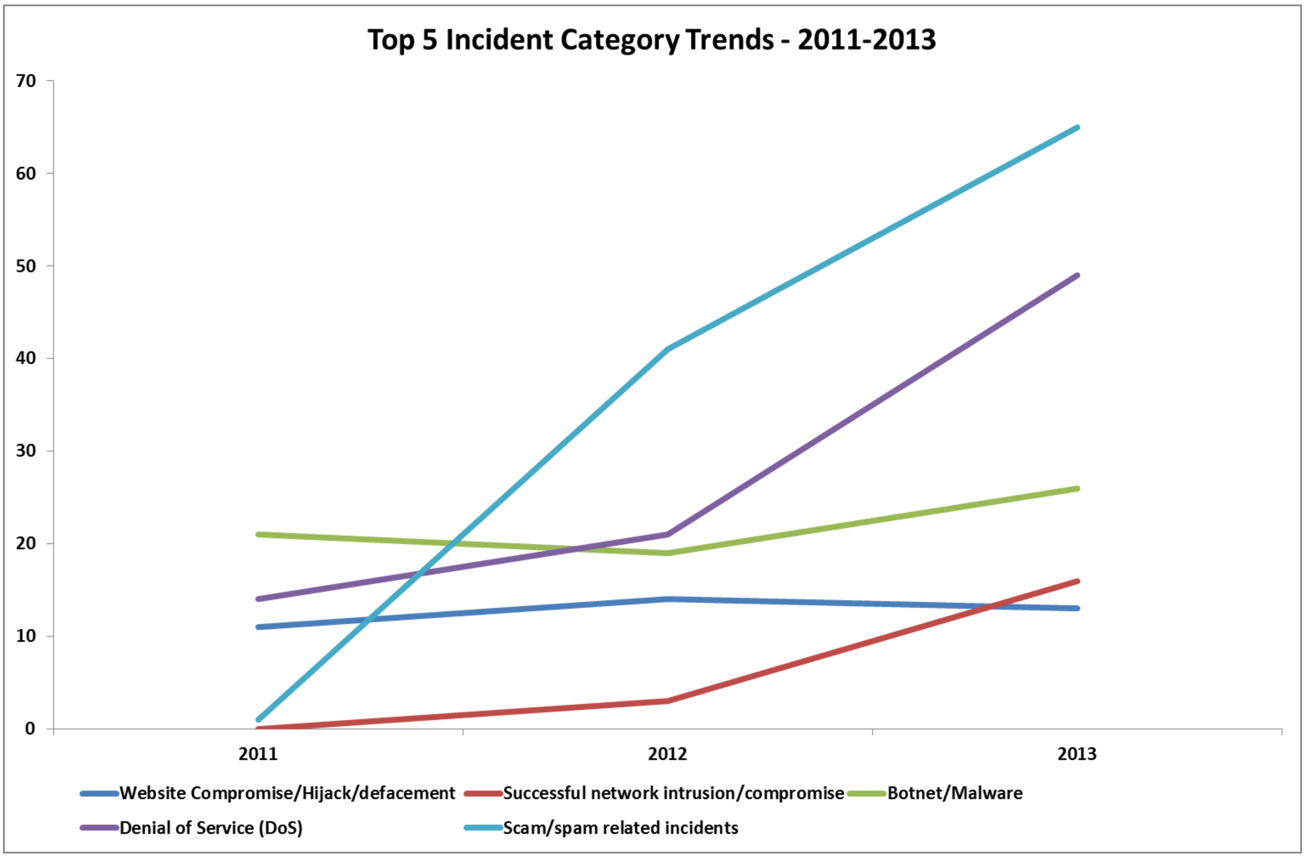


Figure 1.2 highlights the changing trends in reported incidents.

Case Study 1: Successful Spear Phishing Compromise

A number of New Zealand organisations reported receiving spear phishing emails. Spear phishing emails are targeted emails which try to pass themselves off as legitimate emails with attachments containing malware, and are designed to trick the recipients into opening them. Upon doing so, malware is automatically installed on the user's computer and can then be used by an attacker for further compromises.

In one case, a targeted spear phishing email containing a malicious .pdf file was sent to a number of email addresses for an organisation. Several recipients opened the attachment which then exploited a known vulnerability to install malware on the user's accounts.

Once the malware was installed, the perpetrators were able to access the network and get greater privileges to increase their access across the network. Ultimately they were able to collect and then extract sensitive information from the organisation.

Incident Attribution

Specific attribution of incidents can be problematic due to common measures used by malicious actors to mask their identity and location. Information sharing between the international IT security community can help provide a level of attribution.

In 2013, NCSC identified the bulk of reported incidents (63 percent) originated from an overseas source. Nearly a third of the incidents reported (31%) involved incidents originating from domestic sources. 6% of incidents were unable to be attributed to a specific origin.

Fig 1.3

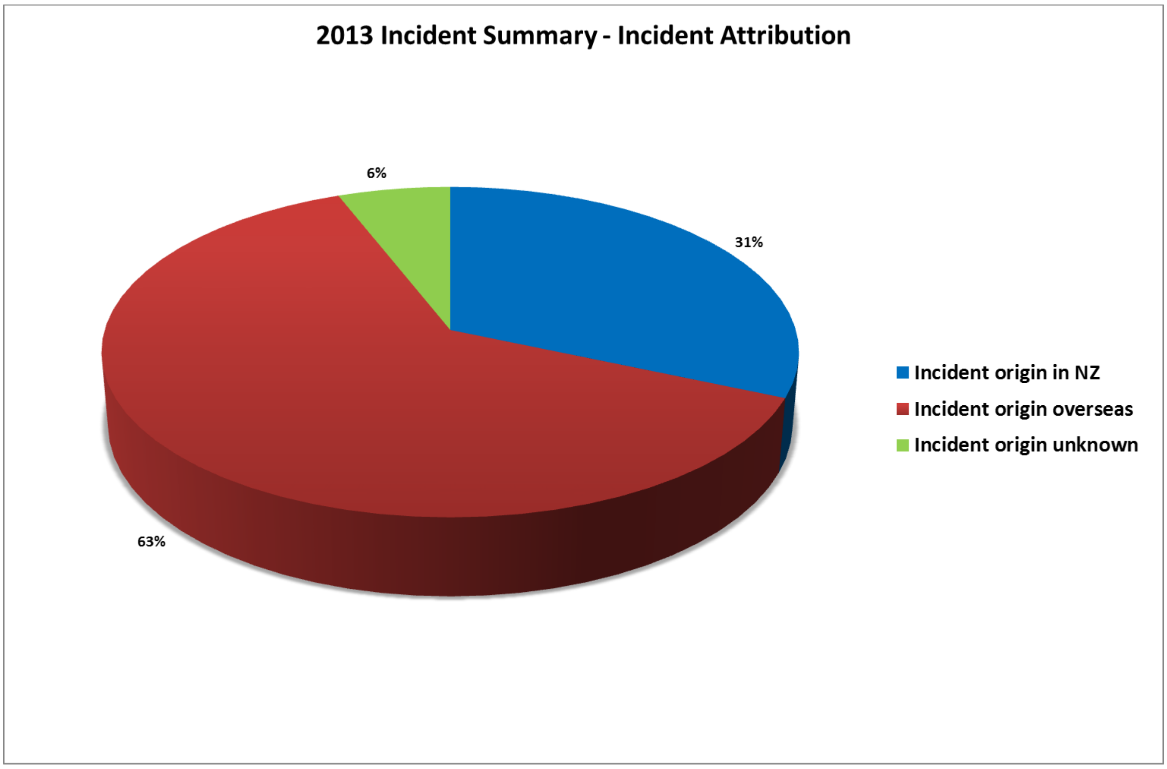


Fig 1.4

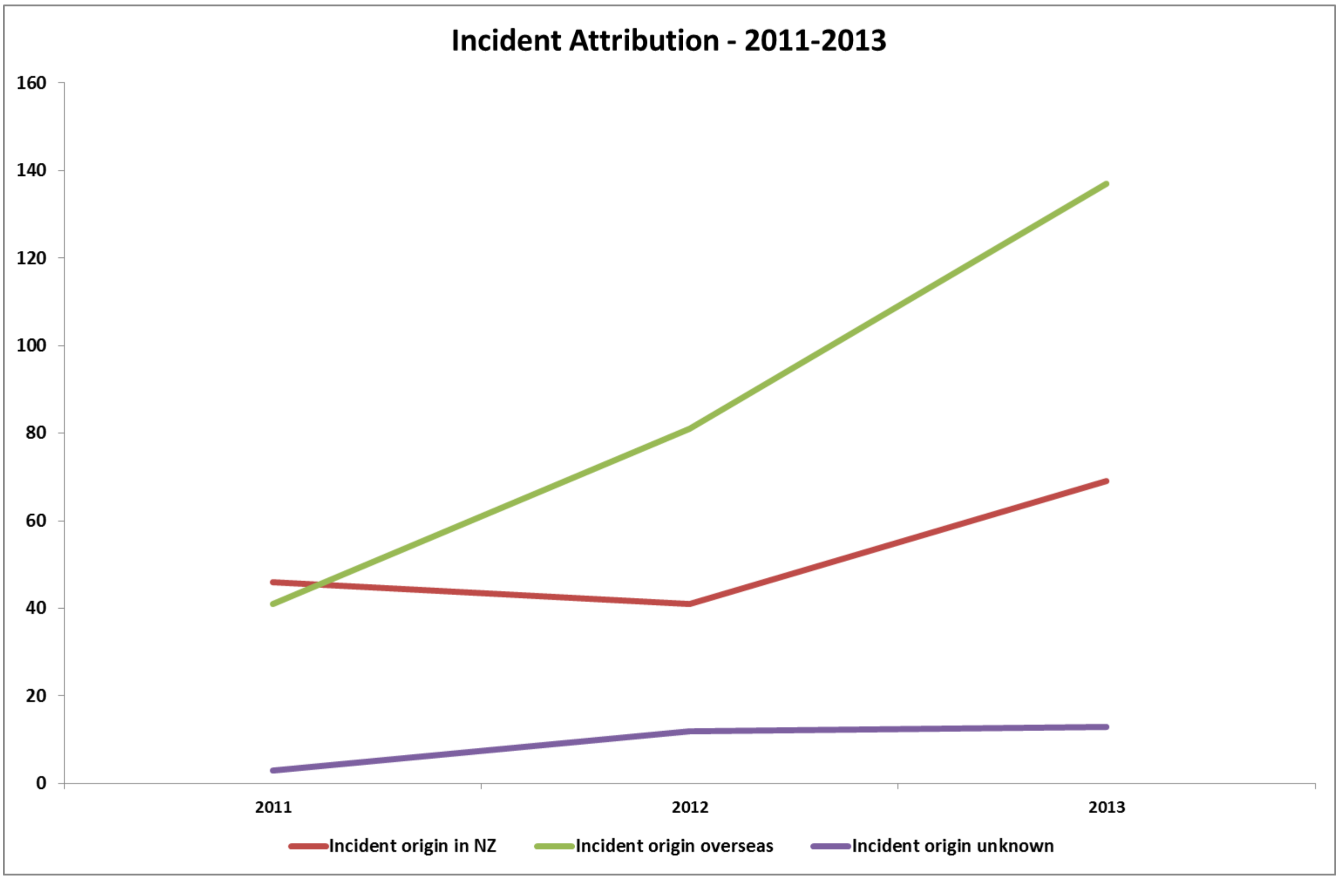


Figure 1.4 highlights the changing trends in incident attribution.

Case Study 2: Spoofed Email Address

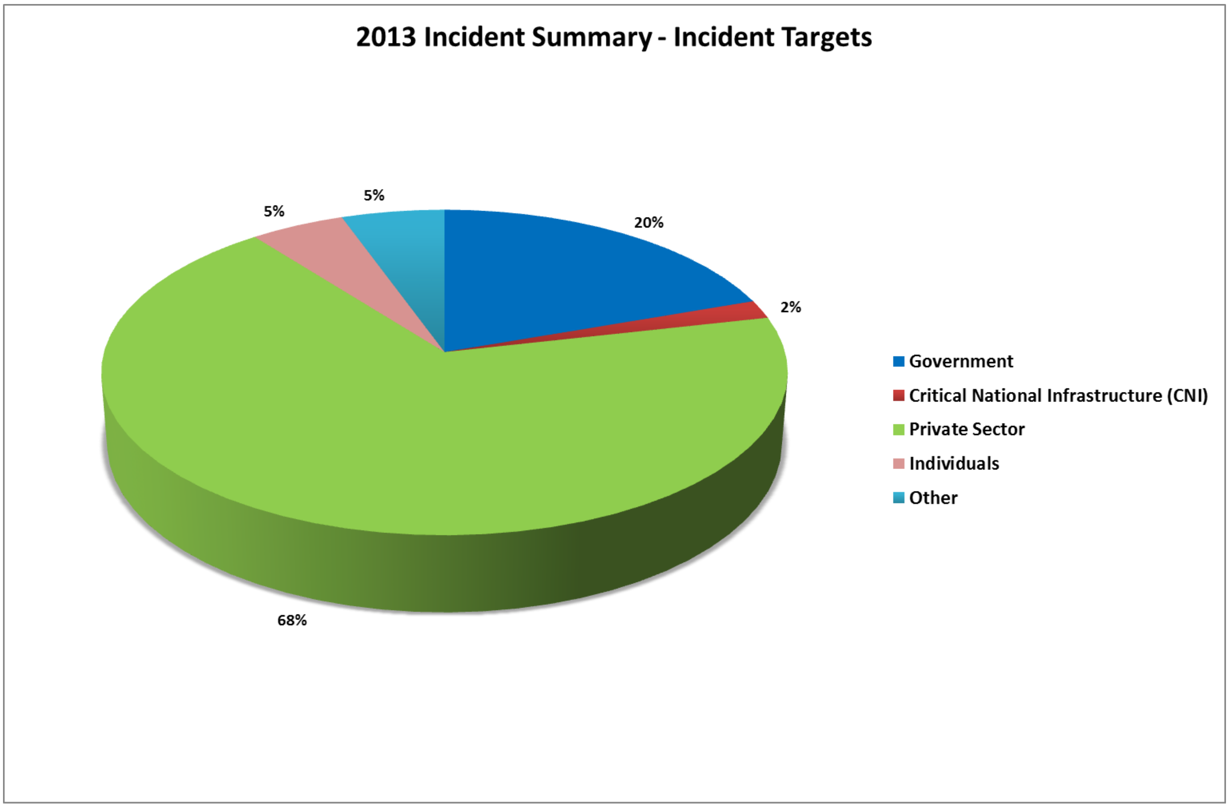
Private sector organisations reported receiving emails from scammers pretending to be employees. These “spoofed emails” were set up by scammers who were able to identify employees from the organisations’ open source information.

The attackers used these names, or similar variations, to establish free email accounts. These web-based email addresses were then used to send emails to colleagues of the legitimate employees, requesting funds be paid on behalf of the organisation to bank accounts operated by the scammers. The organisation suffered financial loss as a consequence.

Incident Targets

The majority of incidents reported in 2013 were targeted towards the Private Sector (68%), followed by the Government (20%), Individuals (5%) and critical national infrastructure, (2%).

Fig 1.5



Case Study 3: Ransomware Attack on Company

A number of “ransomware” reports were received in 2013. In one case a small business reported they had received emails from outside of New Zealand threatening to disable their business unless funds were paid.

When no funds were paid the email senders – we call them threat actors – compromised the business’s servers, installed malware which encrypted their files, causing the owners to lose access to their systems.

Eventually the organisation was able to restore its network using historic back-ups, however they lost many recent records and were unable to conduct business for several days resulting in subsequent financial losses.

Fig 1.6

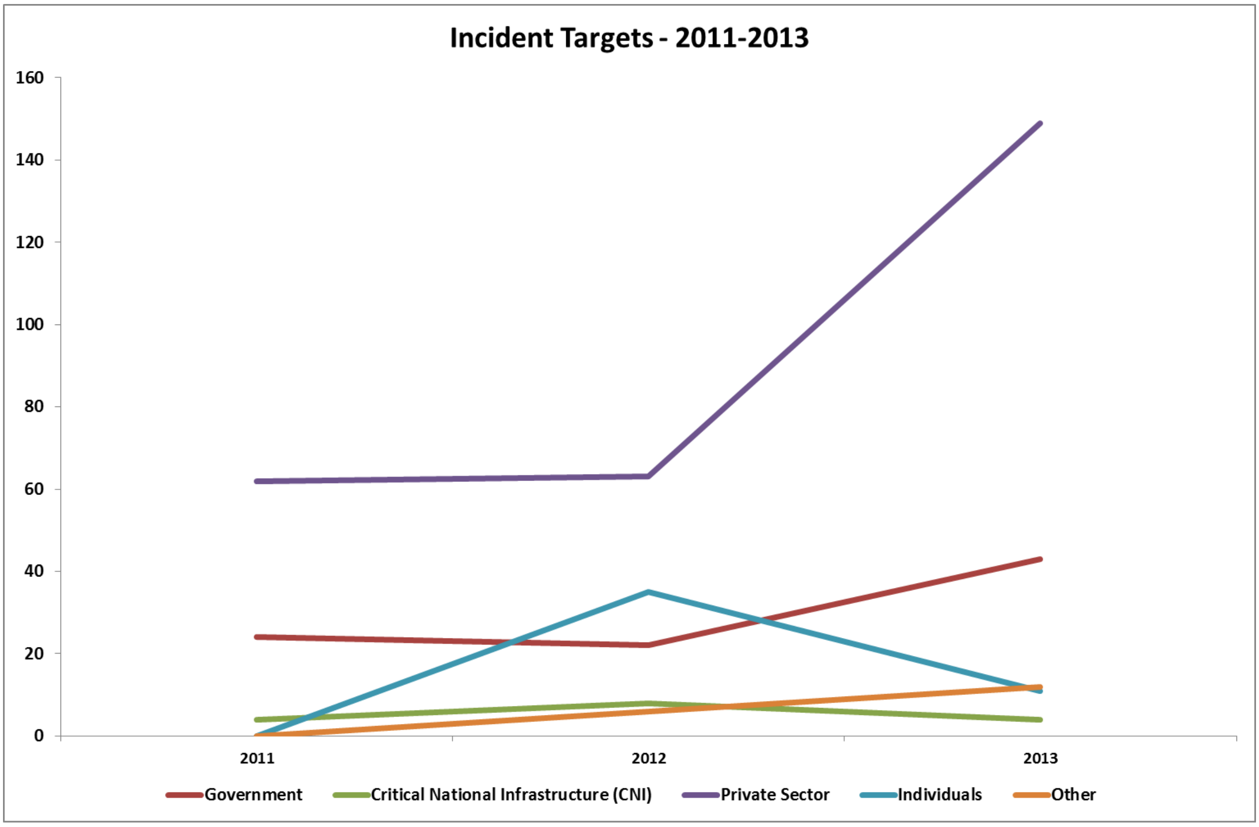


Figure 1.6 highlights the changing trends in incident targets.

Concluding Remarks

While this report is based on a relatively small number of recorded incidents (219) in 2013, these incidents do fall into the more significant categories of cyber intrusions occurring in New Zealand's cyberspace.

The National Cyber Security Centre's on-going focus will remain the protection of core Government networks, the systems which support critical national infrastructure, and engagement with industry and business to protect intellectual property and economic assets.

The National Cyber Security Centre interacts with other agencies, such as New Zealand Police National Cyber Crime Centre and the Department of Internal Affairs, international Computer Emergency Response Teams (CERTs), and non-government organisations, such as Netsafe, to help address the wider range of cyber threats.

Contact Details

If you or your organisation has experienced a cyber-security incident, this should be reported to the NCSC, as quickly as possible.

All incidents must be reported via a completed Incident Reporting Form which is available on the NCSC website at: http://www.ncsc.govt.nz/incidents.html. Completed forms should be emailed to incidents@ncsc.govt.nz and if required you can speak with the NCSC directly on (04) 498-7654. All reports received are held in confidence.