Eliminating phishing and whaling attacks.

Protecting organisations from email domain spoofing with DMARC.

Research paper
September 2020

Authors
Thom Hooker
Roy Foubister

SMXEMAIL.COM

Foreward

Research by email security provider SMX has shown that ANZ businesses and government agencies remain vulnerable to email attacks using spoofed email addresses thanks to the low uptake or incorrect implementation of DMARC (Domain-based Message Authentication Reporting and Conformance).

As modern email gateway solutions have tackled the bulk of malicious emails, cyber criminals have become more sophisticated in their approaches, marrying clever facsimiles of genuine emails with domain spoofing so that the email appears to originate from the business or individual it claims to represent. Even users aware of email security issues can be fooled by the appearance of a legitimate sender address, leading the victim to either click on a malicious attachment or respond to the request contained within.

$14.5m - $60m in losses

In 2019 financial losses due to scam and fraud totalled $14.5m in New Zealand and $60m in Australia

What's at stake.

New Zealand

According to CERT NZ, **financial losses due to scam and fraud totalled $14.5 million in 2019,** with **87% of that being due to email fraud.** There was a **25% increase in phishing and credential harvesting incidents** compared to 2018. Ransomware attacks, which are typically launched via email, are particularly threatening, with CERT NZ reporting last year that 70% of the ransomware attacks reported to the agency since it was set up led to some form of loss for the victim. Apart from the financial losses, organisations exposed user data and suffered reputational damage as a result.

Australia

According to the Australian Competition and Consumer Commission (ACCC) and Scamwatch, **financial losses due to email scam and fraud totalled $60 million in 2019 and is on the increase.**

This is further supported by the Australian Threat Report of CIO's that identified **phishing attacks are the top cause of data breaches.**

The DMARC solution.

A key part of the solution to this problem has existed since 2015. DMARC, when properly implemented, filters incoming email and verifies whether an email was sent by the purported sender. The result is that no matter how well constructed the impersonation of a company or individual is, the email filtering program is able to detect and reject the malicious email.

The SMX research shows that despite many of the entities understanding the value of DMARC, uptake of it remains low with both business and government across ANZ.

Despite the security advantage DMARC offers, uptake of it remains low across both business and government in ANZ. This is putting entities at risk of significant financial and reputational losses while running the risk of a privacy breach, all originating from an email scam."

- Thom Hooker, SMX co-founder, director and research lead.

Who's exposed?

New Zealand

The research found that while one third of the top 100 New Zealand companies have some form of DMARC record many of those were either still at the experimental phase or even worse had misconfigured records. **Only 8% of top 100 New Zealand companies could be said to have a solid DMARC implementation.**

The results within government agencies, where large amounts of personal and business data resides, is worse.

Looking at the DNS records of all 372 NZ government agencies found that **74 agencies have some form of DMARC record** with large numbers of misconfigured or invalid records amongst them. Of the 74 agencies with some form of DMARC **only 12 are configured to reject email, with another five configured to quarantine emails that breach their policy.**

Australia

Australian Federal agencies are only slightly ahead of New Zealand. **Of 187 agencies 103 have some form of DMARC record although only 32 (17%) have a record in enforcement mode. 71 (37%) have DMARC but are effectively taking no action** (including no reporting) while **84 (44%) have no record at all.**

Why does it matter?

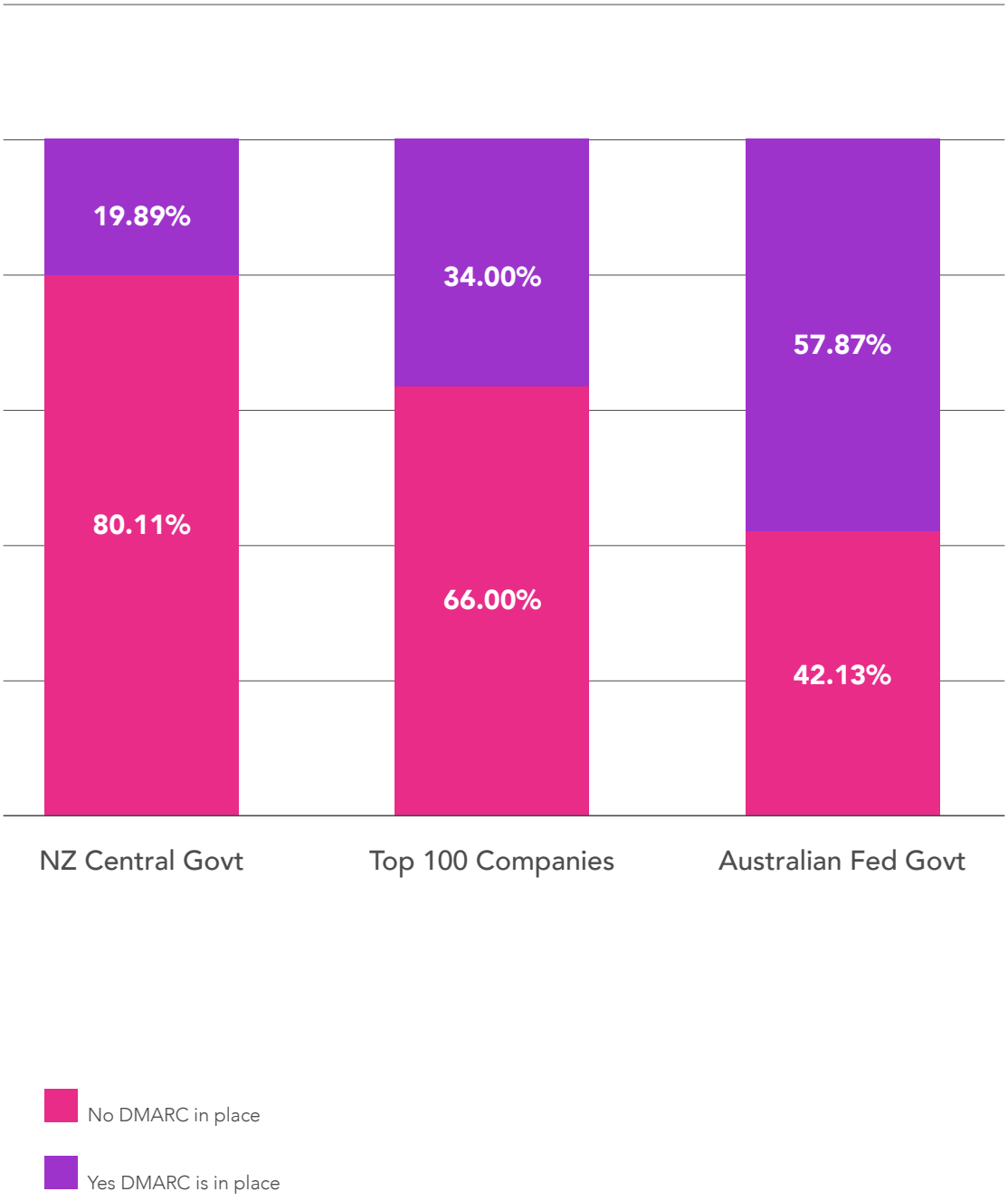
Poor DMARC uptake continues to put businesses and individuals at risk of financial or data loss while government agencies run the risk of exposing personal data due to a privacy breach originating from an email scam.

Both the Australian federal and New Zealand central governments are placing increased focus on data privacy as evidenced by New Zealand's Privacy Act 2020 and Australia's Privacy Act 2018 amendments. So it is imperative that both businesses and government agencies take all appropriate measures to protect personal data held not only in their servers, but also via email.

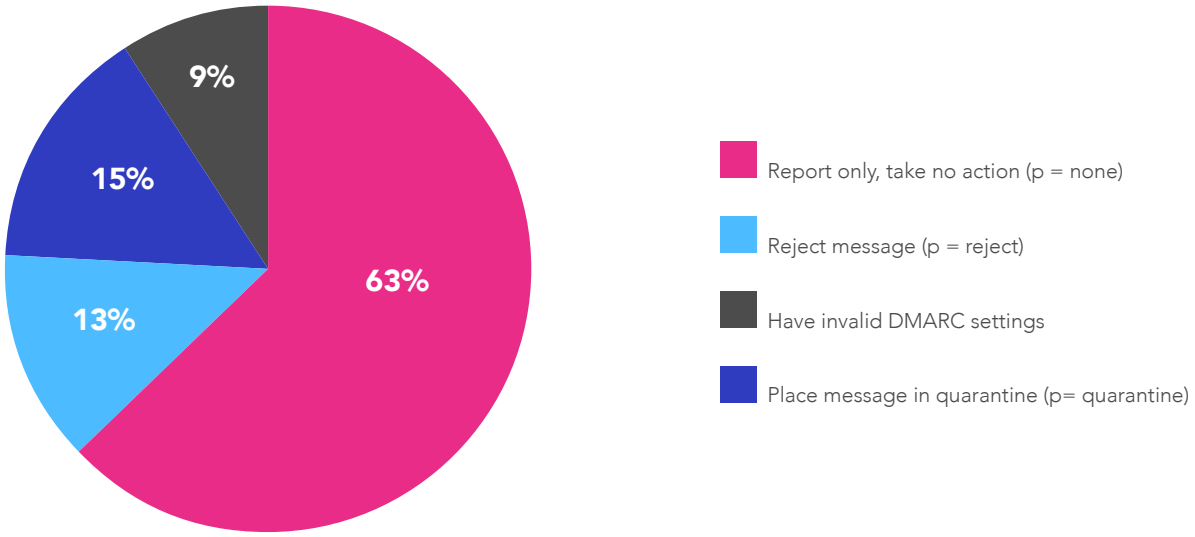
55%

Only 55% of all Australian Federal agencies have some form of DMARC record with large numbers of misconfigured or invalid records amongst them.

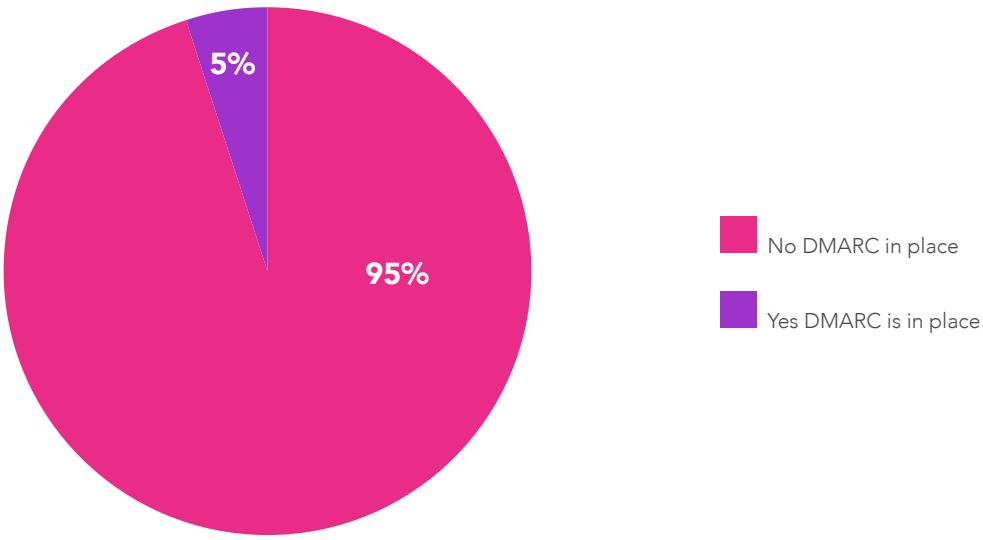
DMARC Use by Organisation Type



DMARC Setting Use



How Many Oranisations Currently Using DMARC



Only 20%

of all New Zealand government agencies have some form of DMARC record with large numbers of misconfigured or invalid records amongst them.

Key takeaways

Why the reluctance?

It's just the way it is.

In-market feedback shows part of the problem is a perception that email is inherently insecure. Therefore there isn't a way to stop spoofing attacks beyond good vigilance and standard email filtering tools. This is simply not true.

DMARC is now a hygiene-level policy that should be implemented. It fundamentally changes that situation, providing organisations with a technical solution that establishes the legitimacy of an email beyond doubt and provides an opportunity to reject or quarantine accordingly.

Proof-of-value is lacking

Other in-market feedback indicates that many of those who have previously implemented DMARC either failed to implement it fully or made mistakes in doing so, both of which led to sub standard results and a perceived lack of value.

It's time.

Since DMARC was introduced in 2012 there have been vast improvements made in supporting IT professionals with its implementation. Given its vital role in helping fight email-based cyber threats, it's time to give it another go to protect organisations, reputations, financial interests and both clients and constituents.

SMX offers DMARC support and advisory services for our customers.

Get in touch with your SMX Reseller, Account Manager or drop us an email at emailsupport@smxemail.com

SMX is an email archiving, security and management provider, used across Australia and New Zealand by some of the most proactive cybersecurity IT leaders and managed service providers.

Established in 2005, we work with clients ranging from large ISPs such as Spark, to government agencies such as the Department of Family and Community Services and Waikato District Health Board, to large businesses such as Fisher & Paykel Finance and The Northcott Society.

Our cloud-based email security and archiving platform, encompassing SMX SEG, admin portal and Accelerate email archiving, is purpose-built to repel whaling, phishing and spam attacks before they hit a network. Additionally they simplify the email management and archiving processes leaving more time for IT teams to spend on greater value tasks and providing peace of mind about email attack vectors.

Contact us at smxemail.com
or connect with us on LinkedIn or Twitter.