OUTFOX

MSP INSIGHTS ON CYBER RESILIENCE

Authors: Wendy Bennett & Jan Thornborough, Outfox Ltd

www.outfox.co.nz

Foreword

Jan Thornborough
Managing Director
Outfox Limited

Wendy Bennett
Director
Outfox Limited

Cyber resilience is a critical challenge for small to medium sized enterprises (SMEs) in 2024. This year's review of MSP Insights on Cyber Resilience sheds light on the hurdles MSPs face in addressing the cybersecurity gaps within the SME sector of New Zealand's economy. Larger organisations and government bodies have the resources to strengthen their resilience, however SMEs often rely on MSPs to manage this vital aspect. With cybercrime on the rise globally, New Zealand is no exception to this trend. At Outfox, we've witnessed firsthand the difficulties MSPs encounter when their efforts to improve clients' cyber resilience are met with indifference or a lack of understanding about the growing threat. MSPs are increasingly frustrated by their clients' reluctance to take responsibility for their own cyber resilience, often expecting MSPs to shoulder the burden of safeguarding their business against cyber-attacks.

This paper draws on our research and experiences from collaborating with MSPs to deliver cyber resiliency services to SMEs both in New Zealand and abroad. It offers valuable insights into the range of cyber resiliency services available to SMEs and evaluates the effectiveness of these in bolstering the resilience of this vital sector of New Zealand's economy.

Executive summary

Neglecting cyber resilience leaves SMEs dangerously exposed to escalating threats.

In today's digital economy, reports of cyber-attacks crippling organisations occur daily. It affects all industries and organisations of all sizes. No industry, or organisation is safe.

While large organisations are starting to invest in improving their cyber resilience, SMEs are getting left behind.

The high cost of cybersecurity tools and the scarcity of cybersecurity experts means SMEs need to rely heavily on their MSP to provide the layers of protection essential for surviving in the digital jungle.

MSPs are taking a hard line.

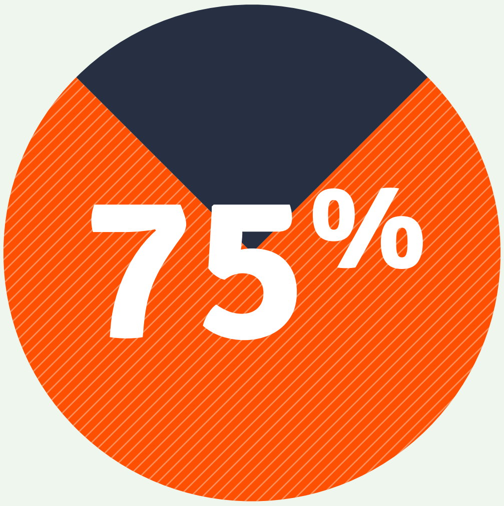
Recent cyber-attacks on MSPs have galvanized some to draw a line in the sand. They offer a mandatory minimum-security package to new customers. Some have even stopped working with customers who refuse this essential level of protection. This move is one of self-preservation as much as it is setting a benchmark of minimum standards.

Customers abdicate their cyber resilience responsibilities.

2023 was the worst year for cyber-attacks globally. Yet, many MSPs indicated there was no increased expenditure by their customers on cyber resilience in the past 12 months. As cybercrime continues on a steep trajectory, SMEs are becoming increasingly vulnerable to attacks.

Technical cybersecurity offerings are only part of the solution.

Cyber resilience requires attention to three essential elements: people, processes, and technology. In a time where cybersecurity expertise is scarce, more MSPs are turning to collaborative partnerships to access the skills needed to strengthen their cyber resiliency offerings



75% of the respondents employ 20 or less staff. Some manage from 100 to 500+ customers.

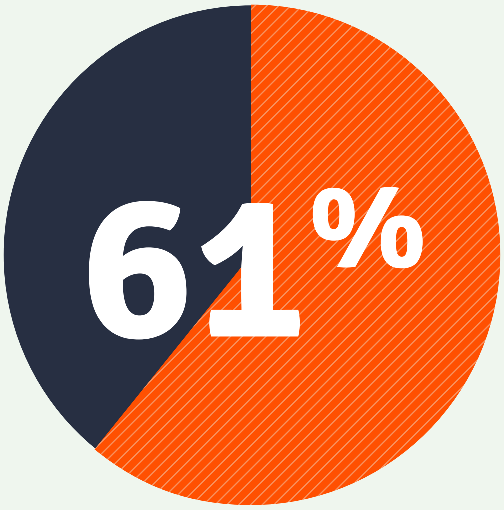
Fit for purpose cyber-resilient services and security architectures are essential for SMEs to operate safely in today's digital business economy. But with the cost of sophisticated security solutions out of reach for most SMEs, coupled with a severe shortage of good cybersecurity talent, MSPs have the unique role to play in the delivery of cyber resilient solutions to their clients.

New Zealand is a nation of small businesses, and MSPs are no different. The majority of the respondents to this survey were small MSPs i.e. organisations with 20 or less staff. We focused on MSPs that serve sectors often overlooked by larger cybersecurity companies. Most of the MSPs we interviewed support a diverse range of clients, from non-profits to multinational corporations, with SMEs representing the largest portion of their customer base.

> **"Key indicators for systemic cyber resilience include the quantity and quality of industry collaborations, the effectiveness and clarity of regulations, the maturity and accessibility of the cyber insurance market, and the extent to which organizations understand cyber risk coming from their own supply chains and third-party relationships.**
>
> **When an organisation finds common ground In its relationship with its suppliers, regulators, government agencies and industry peers, it creates a more resilient digital landscape. Conversely, an organisation cannot truly be resilient if the partners on whom it relies on are fragile".**
>
> **World Economic Forum Global Cybersecurity Outlook 2024 Report**

Introduction

In 2024, cyber resilience is a significant challenge for SMEs in New Zealand and globally. As specialists in this field, we've witnessed the rise of cybercrime and the struggles MSPs face in getting clients to recognise and address the issue. To quantify this, we surveyed MSPs across New Zealand. This white paper examines the challenges MSPs encounter in helping SMEs enhance their cybersecurity. While larger organisations have the resources for robust cyber defences, SMEs often rely on MSPs for protection. With cybercrime increasing, it's vital for SMEs to understand and invest in cyber resilience. This paper provides insights from MSPs to better protect themselves in the digital world.

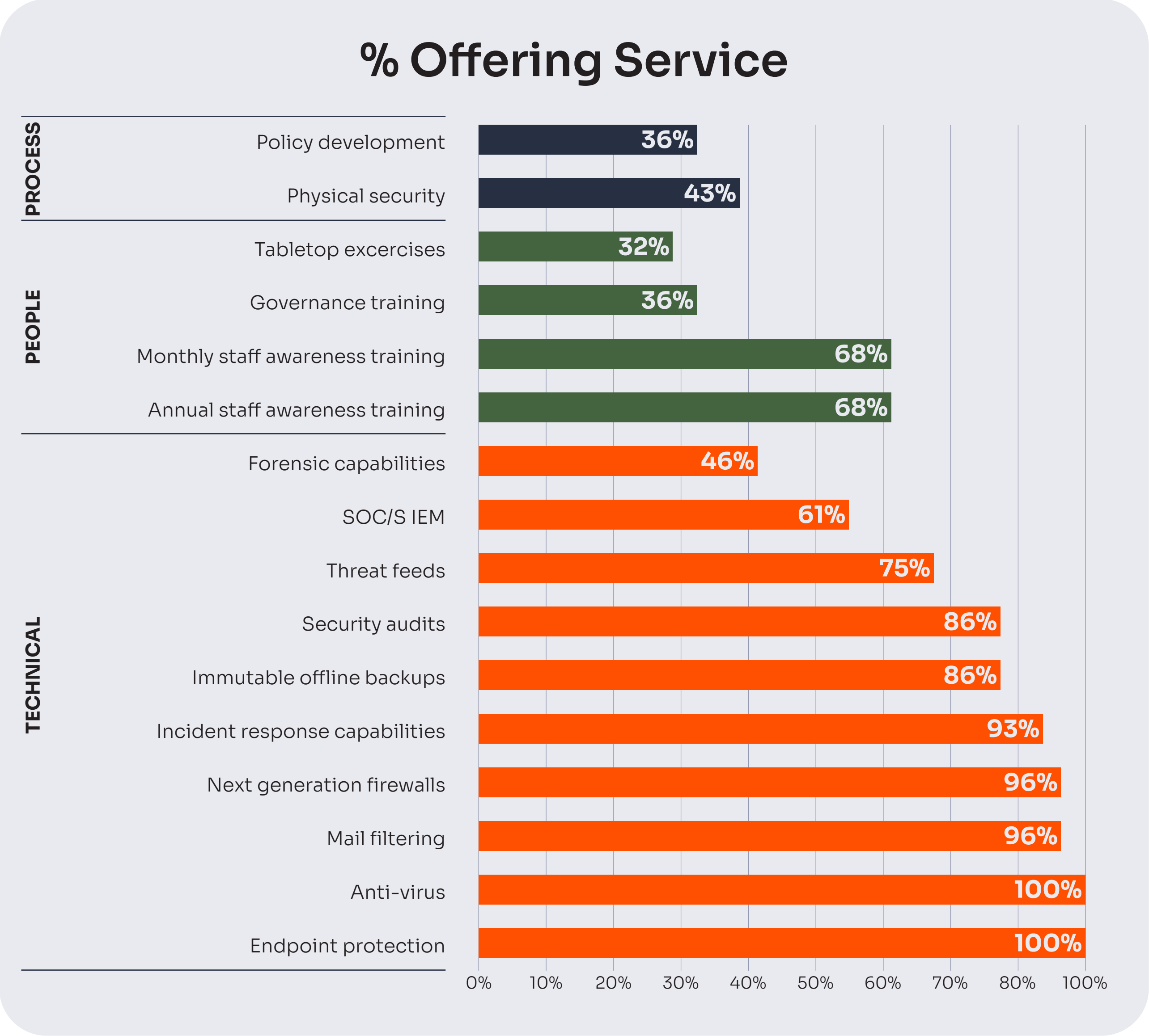


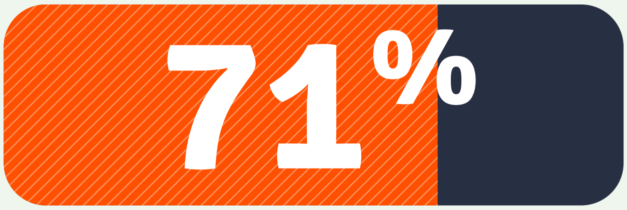
61% of MSPs offer SOC or SEIM capabilities.

MSP service offerings

Achieving cyber resilience requires the alignment of people, processes, and technology. Many of the MSPs we interviewed offer a variety of services, either in-house or through outsourcing to companies like Outfox. Notably, 61% provide a SOC or SIEM capability, which is crucial for detecting cyber-attacks. 46% offer forensic capabilities to determine how and when an attacker may have breached their systems. The services least offered are cybersecurity policy development and educating people. MSPs that offer services in all these areas have a competitive advantage.

Often the skillset at MSP's are more aligned to the delivery of technical services. MSPs that collaborate with Outfox get access to cyber resilience expertise focused on the areas that they are often not resourced for. This enables them to offer a comprehensive cyber resilience portfolio with added value in a competitive market.





71% of MSPs offer a minimum level of cybersecurity protection.

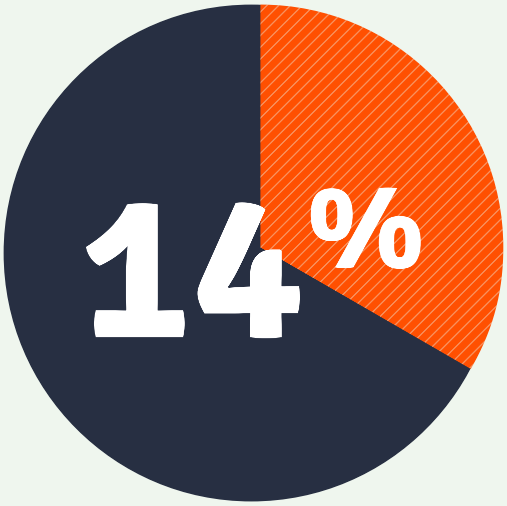
Security levels available to SME

71% of MSPs offer a minimum level of cybersecurity protection that includes antivirus, mail filtering, endpoint protection, and next-generation firewalls. A notable trend that surfaced is that some MSPs are now refusing or discontinuing service to customers who do not adopt this minimum-security suite. MSPs that do not offer minimum security suite, indicated they do the best they can to tailor services for clients based on what clients can afford.

This trend is a positive and necessary step toward enhancing overall security. By enforcing a minimum cybersecurity standard, MSPs are ensuring that all clients, regardless of size or industry, have a basic level of protection against increasingly sophisticated cyber threats. This approach not only helps protect individual organisations but also strengthens the broader ecosystem by reducing the risk of vulnerable entry points that could be exploited by attackers., By refusing to work with clients who do not meet these minimum requirements, MSPs are sending a strong message about the importance of cybersecurity. This proactive stance encourages businesses to take cybersecurity more seriously, ultimately contributing to a more resilient and secure digital business ecosystem in New Zealand. This approach must be balanced with education and support. Some clients may lack the resources or understanding to implement these measures, and MSPs should work with them to bridge these gaps, rather than simply cutting ties. This combination of enforcement, education, and support can lead to a more secure and informed client.

Trusted partners

We make it easy for SMEs to become cyber resilient. Outfox specialises in getting customers across the line on the importance of being cyber resilient. We educate them on the gaps and make it easy for them to improve their cybersecurity with the help of their MSP.



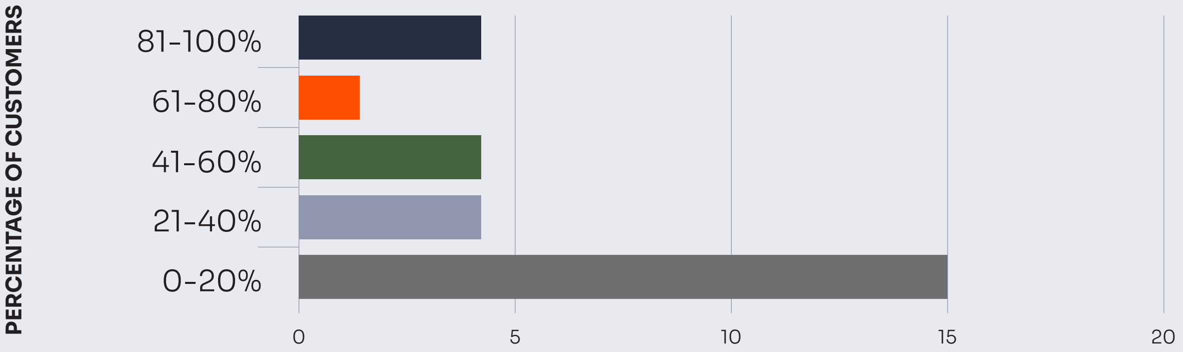
Only 14% of MSPs report clients taking up a full protection security suite.

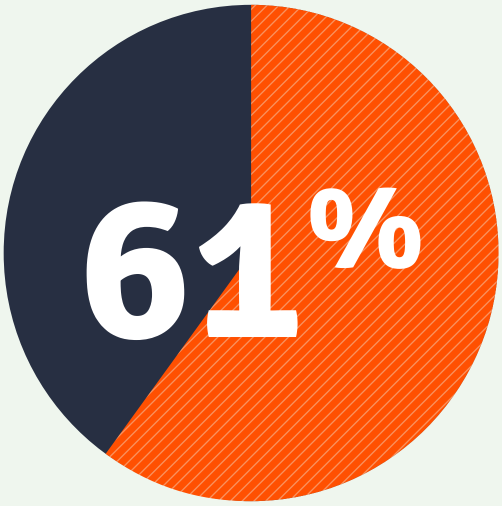
SMEs are lagging behind

Globally, there is looming cyber inequity as the tech landscape rapidly evolves . There's a growing divide between cyber-resilient organisations and those that aren't, especially among SMEs. The rising costs of cyber services, tools, and expertise are hindering efforts to build a more resilient economy. In New Zealand, while large and Nationally Significant Organisations(NSO's) are enhancing their cyber resilience, SMEs are lagging. This is not from a lack of services available from MSPs. Rather, a reluctance among customers to take responsibility for their own cyber resilience.

This is further emphasised in CERTNZ's latest report on SME cyber security behaviour. They report that only 55% of the organisations surveyed consider cybersecurity a top priority for their organisation right now. Our survey found that only 14% of MSPs reported that 80 – 100% of their customers had invested in a full suite of security measures. They attributed it to their proactive education on the cyber threat landscape and the benefits of better protection

How many clients adopt a full security suite





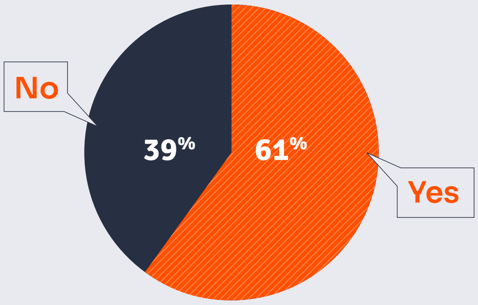
61% of the MSPs provide IT services to critical infrastructure.

Protecting our critical assets

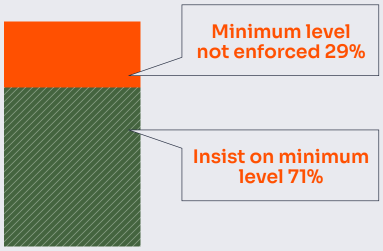
MSPs have another critical role. 61% of them reported that they provide IT services to critical infrastructure. NSOs are those that, if compromised would have a significant impact on everyday New Zealander's lives.

Of concern is that 14% of the MSPS reporting NSOs as customers also indicated that they don't provide a mandatory minimum-security suite. This is not just a lost opportunity for MSPs, it potentially creates a significant risk to the New Zealander economy.

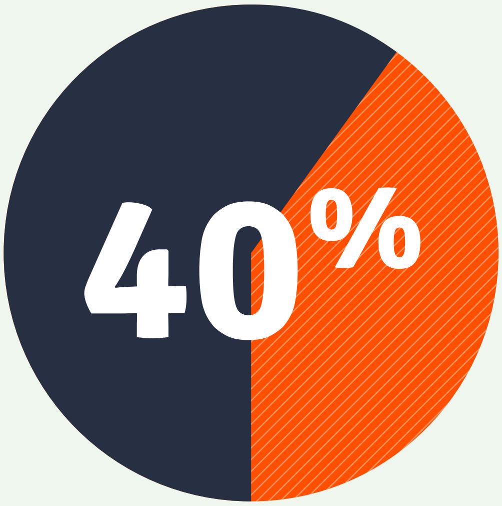
Do MSPs provide critical services to government or nationally significant organisations?



If yes, do you insist on a mininum level of cyber resillience for these customers?



> “Many SMEs pay more for coffee for their staff, than on their cybersecurity.”



22 MSPs indicated that 40% of their clients haven't invested in security in the past 12 months.

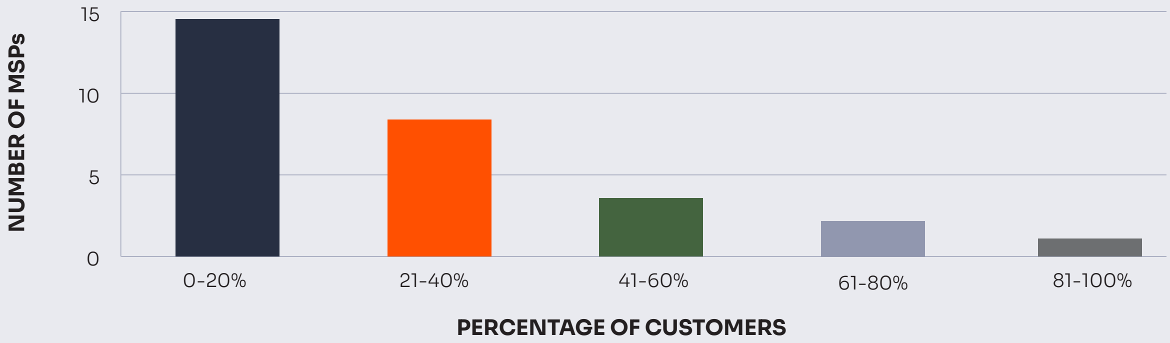
Investment in cybersecurity

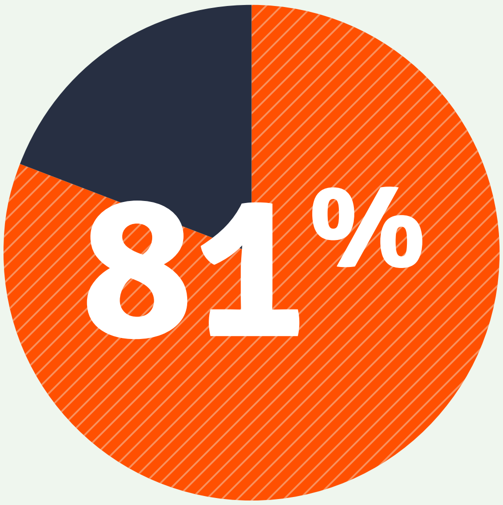
Our research found that only one MSP reported over 80% of their customers had invested in additional cybersecurity this year. They attributed it to their proactive education on the cyber threat landscape and the benefits of better protection.

22 MSPs reported that up to 40% of their customers did not increase their cybersecurity investment in the past 12 months.

Cybercrime has surged, with attackers becoming more sophisticated and persistent, and this trend is expected to continue. As cyber threats evolve and expand, partial security measures are increasingly inadequate. For example, using anti-virus alone is inadequate in today's climate. Without comprehensive cybersecurity, businesses are leaving themselves exposed to escalating risks, which could lead to severe financial and reputational damage.

What percentage of customers that have invested in additional cybersecurity in the past 12 months by MSP





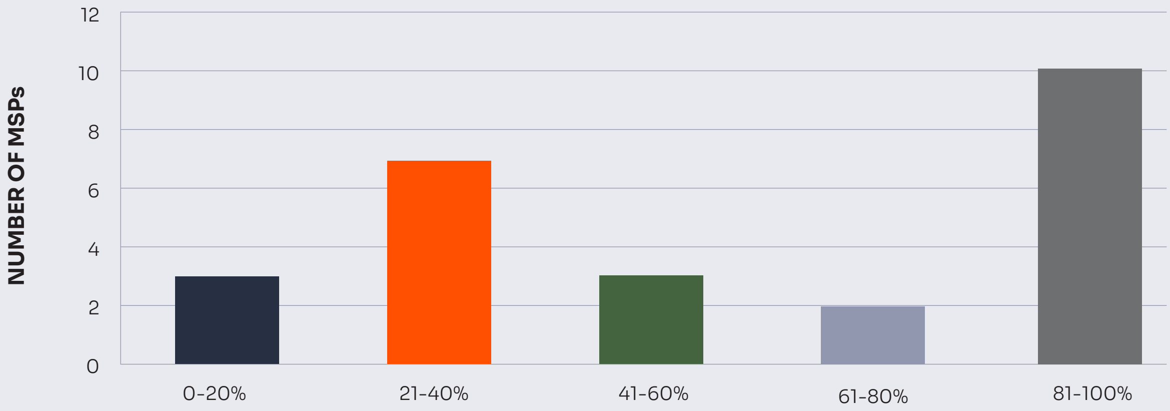
10 MSPs indicated that over 81% of their clients don’t conduct annual reviews of their security.

SMEs ownership of cybersecurity

The gap between the rising threat landscape and the low adoption of robust cybersecurity measures creates a dangerous vulnerability that could be costly to ignore.

Our research and customer interactions reveal that many small to medium organisations tend to fully delegate IT and cybersecurity responsibilities to their MSP. They often lack an understanding of their own obligations to protect their business and have unrealistic expectations of what their MSP can deliver.

What percentage of customers that don’t take cybersecurity threats seriously enough.



53%

53% of MSPs raised concerns about the ambivalence of customers towards cybersecurity.

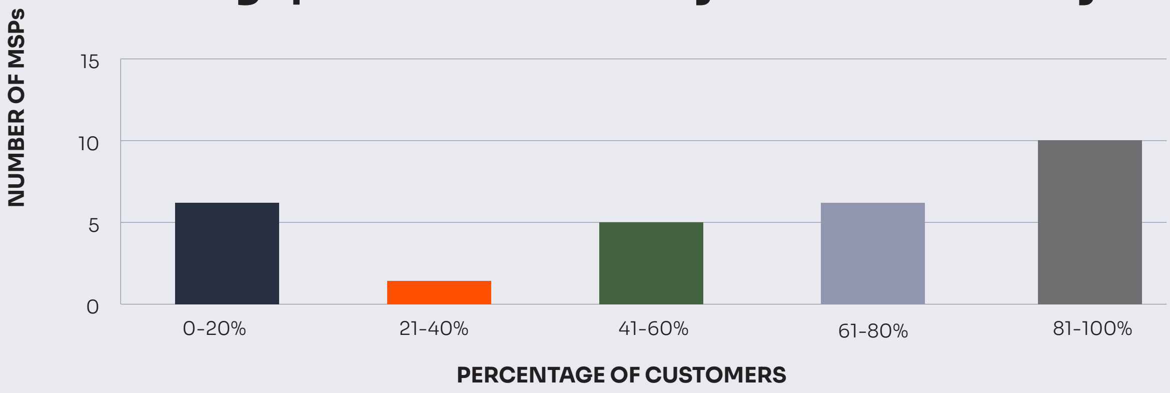
Keeping your eye on the ball

A concerning trend is evident from the survey where 10 MSPs indicated that 81-100% of their customers do not perform an annual Cyber Resilience Warrant of Fitness©. This data implies that many organisations may not be fully aware of the importance of regular security assessments. They also overestimate the extent of the security management provided by their MSPs. Many SMEs we've dealt with think the MSPs are completely responsible for their security management. This is a misguided assumption as organisations cannot abdicate their own business risk. This highlights a need for better education and awareness around the shared responsibility model in cybersecurity, where businesses must be made to be accountable and take an active role in their own protection.

This is even more concerning when we see that a large percentage of the MSPs indicated that their customers seem unconcerned about the current cyber threat landscape. Cybersecurity isn't one-size-fits-all. While MSPs provide critical services, SMEs need to actively participate in securing their own systems. This shared responsibility ensures that both parties are aligned in protecting sensitive data and systems.

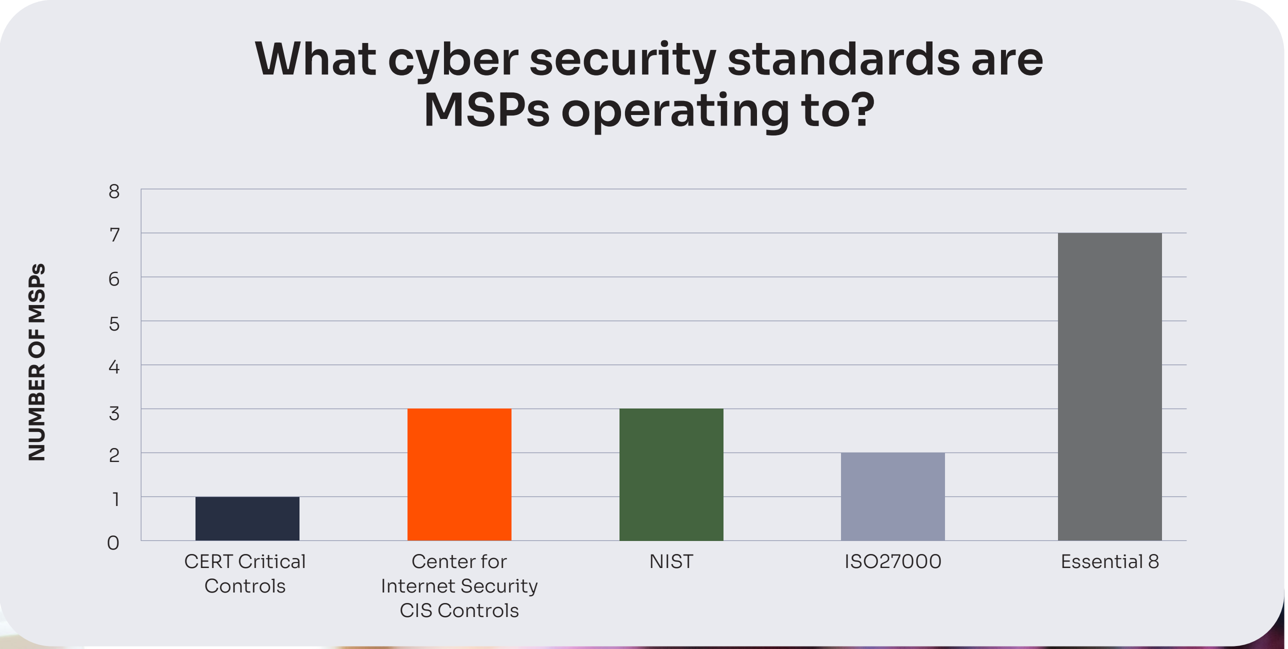
For example, MSPs might manage firewalls, while SMEs focus on employee training and password policies.

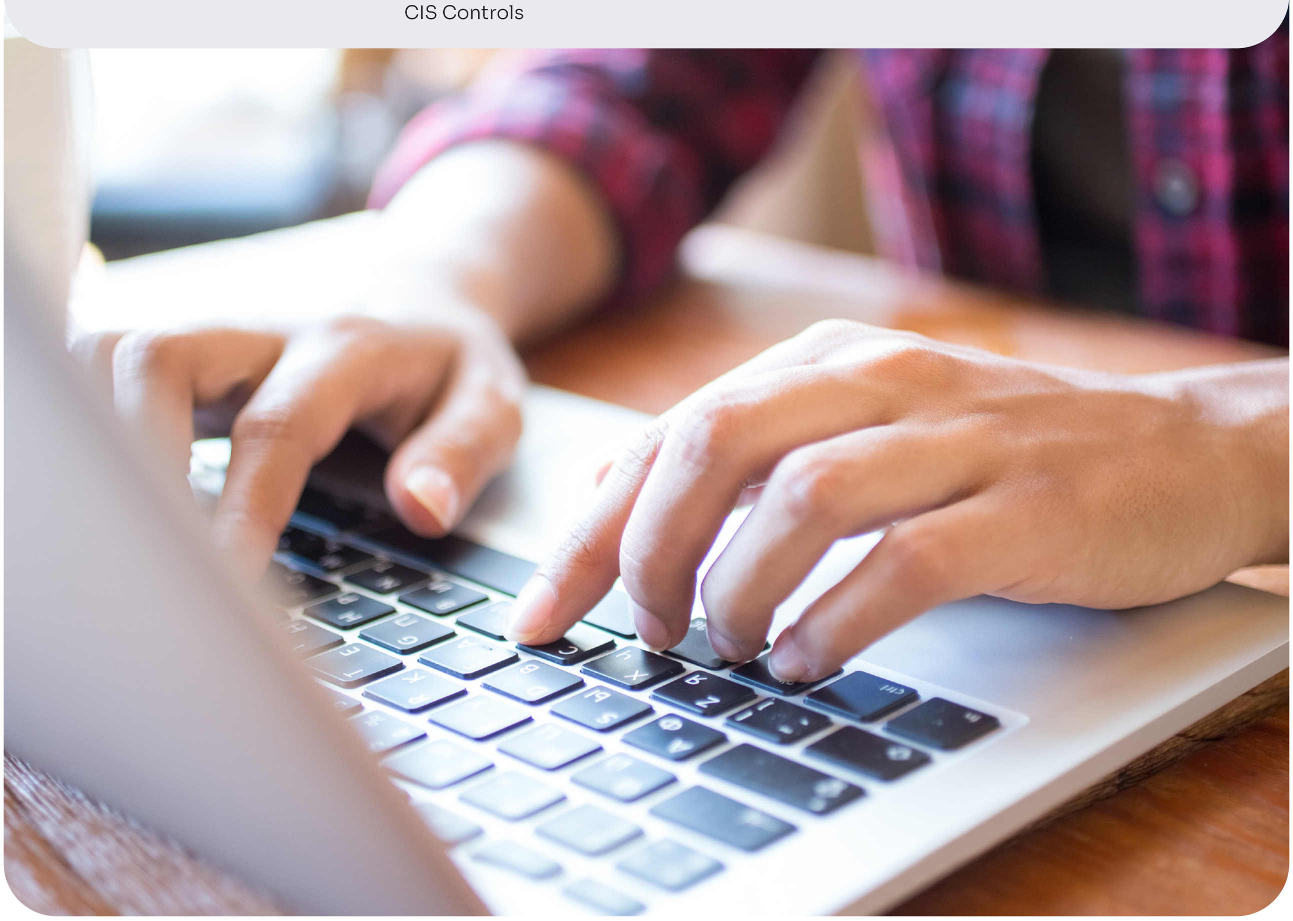
What percentage of customers that don't check the gaps in their security at least annually.



Accredited MSPs

Only two of the MSPs interviewed have invested in achieving an international standard for delivering cybersecurity services. The remainder say they 'align' with other security standards such as NIST, CIS critical controls and Australia's Essential Eight. One MSP aligns to Cert New Zealand's critical controls. Feedback from the MSPs suggests that the cost of achieving and maintaining an ISO accreditation currently outweighs the benefits.


What cyber security standards are MSPs operating to?



Conclusion

Cyber resilience is crucial for SMEs in New Zealand. As cyber threats increase, MSPs are vital in protecting these businesses. This report highlights challenges like clients' reluctance to invest in cybersecurity and a shortage of skilled professionals. By setting minimum security standards and educating clients, MSPs can enhance digital security. Implementing relevant and affordable certifications for MSPs would further improve the sector. Both MSPs and SMEs must collaborate to ensure robust cybersecurity, safeguarding New Zealand's economy against rising threats.

Participants

We would like to extend our sincere thanks to the MSPs nationwide who participated in this whitepaper and generously shared their experiences.

Why have we done this research?

At Outfox, we work with SMEs every day, and we see concerning trends in the attitudes and behaviours of these organisations to being cyber resilient. We wanted to validate those concerns by talking to the MSPs who provide these services.

theta
TechMedics
CREATIVE TECHNOLOGIES
ThinkConcepts
SILICON
OxygenIT
PC HARDWARE
IT LIMITED
OUR CLOUD
NZCS
Business IT Professionals
netcare
Lucidity
Cloud Services
jupiter IT
0800 627 583 help@jupiterit.co.nz
hybrIT
services
exodesk
graphic dimensions
easy-PC
DTSL
caduceus
aiscorp
ONESTOP IT

OUTFOX

0800 940 904
info@outfox.co.nz
outfox.co.nz