|  |
| --- |
| Deakin University |
| New Zealand Cyber Security Strategy |
| Deakin University |
|  |
| **Mohammed Taha Ayaz Merchant** |
| **4/25/2020** |

|  |
| --- |
|  |

Table of Contents

[Introduction 2](#_Toc38751950)

[Executive summary 2](#_Toc38751951)

[Security risk analysis 2](#_Toc38751952)

[Data breaches 2](#_Toc38751953)

[Government and political parties 3](#_Toc38751954)

[Research institutions 3](#_Toc38751955)

[Vulnerabilities 3](#_Toc38751956)

[Ransomware 4](#_Toc38751957)

[Business requirement analysis 4](#_Toc38751958)

[Governance 4](#_Toc38751959)

[Investment 4](#_Toc38751960)

[Supply chain security 5](#_Toc38751961)

[Conclusion 5](#_Toc38751962)

[References 6](#_Toc38751963)

# Introduction

The rapid advancement and the adoption of digital technologies have been seen on a global scale. These technologies aid in fueling up the economy by automating processes that have proven to improve business's productivity, profitability, and speedy development. Moreover, this has enabled firms not only to transition towards automation but also further lead to gathering intelligence, helping them to make decisions effectively.

The rapid growth of technology has also motivated the growth of cyber-enabled threats in terms of scale and scope. Access to confidential information, data, and identity theft and other potentially harmful damage has been reported by organizations that make it essential to uptake stringent cyber-security measures to be able to detect, respond, and recover from such issues.

# Executive summary

Studying the quarterly report of New Zealand cybersecurity strategy for the year 2018-2019, it highlights some key facts that are responsible for such cyber-security intrusions. Firstly, the fast-paced growth of technology has led to an increase in cyber-attacks and still is imminent in the upcoming years. Technology, such as IoT (internet of things), dealing with mass interconnectivity between devices, has led to more gateways for hackers to infiltrate any system or network. Secondly, the rise of malicious attackers continues to rise as new tools and technologies are accessible and usable by almost anyone who doesn't even possess cybersecurity knowledge.

New Zealand sheds light on five areas to work out its strategy to enable New Zealand to thrive online. Finally, the reports concludes that cybersecurity plays an essential part in terms of economic, social, and political factors to maintain the right level of national security and that NZ could benefit from a safe network infrastructure to keep its information private and secure from malicious actors. New Zealand organizations need to emphasize its cybersecurity practices enabling them to create layers of security and, thus, to make it difficult for black hat hackers to succeed.

# Security risk analysis

## Data breaches

New Zealand had reported incidents of data breaches across multiple sectors such as Academia, the airline industry, social media channels, and many others. This breach was performed by state-sponsored cybercriminals, who had the intention to steal personal information for financial gain or their unethical purposes.

However, this poses a high-level risk for individuals who have their privacy compromised and that firms could face reputational damage. As a result, loss in the number of customers and prospects. Data breaches pose a higher risk to these individuals who are targeted continuously through scams or phishing techniques, which were seen by NZ firms.

Similarly, The NCSC uses cyber defense capabilities such as CORTEX to report high-risk cybersecurity threats, including state-sponsored events or risks that may impact New Zealand's cybersecurity well-being (DPMC, 2019). The Cortex had helped identified cyber intrusions one or more of NZs firms through its capabilities. CORTEX is not a ”one size fits all” model (Lisa Fong, 2018), but has the competency to be executed at multiple network points of customers and risk profiles.

## Government and political parties

Governmental bodies consisting of political individuals still face an imminent risk against these cyber-attacks by state-sponsored actors or other black-hat hackers. They may have the intention to interfere between international negotiations or cause potential severity amongst government agencies through espionage that can cause massive havoc throughout any country.

Reports have also found the spread of mass information in an attempt to undermine government processes. For instance, EU member states had their personal information published online throughout December 2018 that included private conversations, financial details, and contacts as well, proving it as a high priority threat to governmental organizations.

## Research institutions

The educational industry is a target for cyber-crime, such as Academia, science, and technology sectors are targeted for continued espionage purposes. These cybersecurity incidents pose a risk to students for having their personal information hacked through these universities.

Moreover, stolen research information on military-based technology from commercial companies and universities was also reported in the NZ reports, respectively. The intention of these cyber criminals by taking research on such advanced technologies is to overcome legal barriers to gain a competitive advantage over other states.

## Vulnerabilities

The NCSC (New Zealand Cyber Security Center) in the year 2018/19 had identified vulnerabilities in their network infrastructure before it was compromised. The malicious attacker had attempted to exploit a weakness in the web server component that is utilized by a large number of firms.

When attacked successfully, it allowed attackers to install malware to open a gateway to compromised servers. The NCSC found that the actor used the access point to dive deeper into the network by executing password generating tools to exploit vulnerabilities across a more extensive network range. The NCSC had worked with other partner firms to determine how deeply the actor indulged into the network, where they reviewed the actor's steps towards exploitation and took remedial advice on securing their network.

Moreover, IoT devices prove to be a threat to cybersecurity attacks and such that are becoming increasingly common. These IoT devices can prove to be gateway points for attackers to access a variety of data. However, awareness seems to be a primary goal for New Zealand cybersecurity strategy, for example, creating educative tools for safer web surfing and making it easier for people to report cyber-crime to get help from governmental organizations.

## Ransomware

Ransomware remains an imminent threat, where cybercriminals are looking forward to achieving financial gain. The NCSC had assisted many firms who were affected by ransomware attacks, having employees email accounts compromised. The year 2018-2019 for NZ was seen as an attack on both the public and private sector firms. Many exploitation incidents had taken place that was due to a lack of multi-factor authentication or unpatched vulnerabilities.

# Business requirement analysis

The NCSC has undertaken data gathering across 250 New Zealand NSOs (Nationally significant organizations). They have identified four key areas that need effective cybersecurity measures to deliver their products and services, also with maintaining long-term relationships with their respective prospects and clients.

## Governance

Governance depicts a senior member of the organization or, in this context, a cyber-security executive who has oversight of cybersecurity issues. An internal team comprising of board members and other executives hold the responsibility for any outcome of cyber incidents that include the impact on any stakeholder or customer confidence (Te Tira Tiaki, 2018-19). They have the objective of aligning organizational goals with cybersecurity as a high priority.

Admittedly, New Zealand faces a cyber-security governance gap where NCSC identifies that 19% of NZ's firms have a dedicated chief information security officer (CISO) in contrast with the other 81% who don't have a responsible senior officer of governing over cyber threats. Firms require the role of CISO due to its effectiveness in dividing responsibilities that can fill the gap for the lack of regular reporting of cybersecurity information.

## Investment

Investing in cybersecurity technology has been seen in New Zealand across multiple areas. These include training IT security staff, new tools and technology, audits and vulnerability assessments. A firm that doesn't undertake cybersecurity investment is vulnerable against cyber-attacks that increase a higher cost in the event of a cyber-incident. NZ has placed its strategy for the years 2019-2023 into improving resilience by ensuring they possess the tools required to counter cyber threats across the system.

## Supply chain security

Outsourcing cyber-security resources might be a short-term necessity for small businesses that lack the investment to obtain new tools and technology, but that doesn't transfer risk. Even if a firm outsources IT services, the board members would be accountable for any outcomes. To understand the risks involved in cybersecurity, having reliable and authentic information is necessary.

Firms relying on third-party services, it is crucial to have cybersecurity reporting when negotiating contracts. Similarly, 64% of the 250 organizations of NZs obtain IT security as part of their vendor contracting process. Moreover, 36 percent of firms are not even sure whether their service providers are providing security services as part of the agreement.

# Conclusion

With the rapid advancement in technology, cyber threats will continue to rise and will bring a negative effect to a countries economic, political, and social factors. Getting the basics right is essential for New Zealand, ensuring that vulnerabilities are sealed within applications and operating systems and undertaking other stringent procedures such as regularly testing, performing backups, securing critical data, and many other cybersecurity reforms.

New Zealand plans to improve upon its resilience by working across multiple sectors, developing informational campaigns, and continue to indulge in its security practices. Moreover, the higher the severity of any malicious activity, the greater it poses a risk towards individuals or organizations, and the higher the costs involved. Both state-sponsored and regular cyber actors are gaining experience with a variety of tools to gain unintended access towards networks

# References

* Enabling New Zealand to thrive online. (n.d.). [online] Available at: <https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf>.
* The National Cyber Security Centre is hosted within the Government Communications Security Bureau Cyber Threat Report Contents Contents. (2018). [online] Available at: <https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Threat-Report-2018-2019.pdf>.
* THINKING AHEAD. BEING PREPARED. Cyber Security Resilience of New Zealand’s Nationally Significant Organisations 2017-2018 NATIONAL CYBER SECURITY CENTRE A PART OF THE GCSB. (n.d.). [online] Available at: <https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Security-Resilience-Assessment.pdf>