delta

Embracing Cyber Risk Management

Issue 10 November 2023

A Broker's Perspective
An analysis of the cyber ecosystem

The Cyber Landscape
The changing face of cyber security in the New Zealand workplace

Risk Management Strategies
How to protect your business

The increasing risks of cyber threats

Delta Insurance released its first cyber white paper in 2018, when supply outstripped demand with a focus on education.

Today, many of those dynamics have reversed.

– Craig Kirk

Group Executive Director, Underwriting

Contents

Amid changing times for cyber insurance industry, demand has never been higher

When Delta Insurance released its 2018 white paper 'The Evolution of Cyber Threats: Embracing Cyber Risk Management', cyber insurance was in a nascent phase, with supply far outstripping demand. Then, the focus from insurers was education – alerting New Zealand's businesses to the reality of cyberthreats and the necessity for the protections offered by an integrated risk management approach in which cyber insurance plays a role.

Today, many of those dynamics have reversed: demand now outstrips supply, while some underwriters are retreating from cyber risk. The education component is largely accomplished, both through the sustained efforts of the technology and insurance industries as well as general awareness driven by an increasingly digitally connected society. Most business owners are also aware of cyber risk, either painfully so as the consequence of a breach suffered personally[1], by their own business, or through the relentless high-profile hacks that have struck major institutions including the New Zealand Stock Exchange[2], the Waikato DHB[3], or the recent incident affecting multiple government agencies via managed services provider Mercury IT.[4]

With the increasing severity and prevalence of attacks in recent times, the local cybersecurity landscape has certainly influenced cyber insurers. While it is the observation of some in the technology field that a poor cybersecurity posture is a sure way for a business to lose a lot of money fast, the same can be said for cyber insurers: poor pricing of risk, or poor risk assessment, loses underwriters a lot of money fast.

Today, running a sustainable and profitable cyber insurance book is more challenging than ever. Creating and delivering profitable cyber insurance solutions demands a deep and thorough understanding of both the insurance business and the technology environment. While most underwriters have no issue with the former, the latter is a more daunting prospect: information technology is a bewilderingly complex and diverse field, with practically infinite specialisations, all of which are impacted by cyber risk.

'Poor pricing of risk, or poor risk assessment, loses underwriters a lot of money fast'.

'Today, running a sustainable and profitable cyber insurance book is more challenging than ever'.

The reality is that with complexity comes opportunity for cybercriminals, who need only focus on a single weakness, exploit or hack within their area of specialty. Their adversary, the defender of the enterprise (be it a major institution or a small local business) must guard against every possible potential threat. After all, the chain is only as strong as its weakest link.

This by no means indicates an inability for the successful and sustainable provision of cyber insurance solutions. What it does confirm is at least two factors: one is specialisation; the other is the necessity of accurate risk assessment, including only taking on clients with demonstrably suitable cyber security postures. In other words, businesses are only insurable if they show capable risk management, encompassing the reasonable protection any organisation should have as a baseline measure against cyber threats that cover their people, process and technology.

This in turn depends on a tightly integrated supply chain, from underwriter through broker, and on to the end customer. In addition to an assessment of the risk exposures faced by New Zealand's organisations, this white paper examines risk management and how you can help potential cyber insurance customers secure cover as an integral component of their strategy.

Reading and sharing the information in this document is intended to help brokers and insured parties understand the risks, the realities and the nuances so every organisation can achieve the necessary level of robust protections. This not only aids in securing cyber insurance, but also strengthens defences against incessant cyber-attacks. After all, as is always the case with cyber breaches, prevention remains a far preferable alternative to cure.

– Craig Kirk, Group Executive Director, Underwriting

Case Study

A major breach of a large medical provider... and Delta's response

'The hackers moved steadily throughout the organisation's data assets, successfully exfiltrating thousands of private medical records to be held for ransom'.

Like many cyber attacks, it started with a tiny gap in the organisation's defence. By compromising the Citrix credentials - a remote access software – hackers were able to gain access to the system of a national medical provider.

As the sophisticated targeted attack unfolded, it became clear that potentially hundreds of thousands of New Zealanders could be affected. The hackers moved steadily throughout the organisation's data assets, successfully exfiltrating thousands of private medical records to be held for ransom. On exiting, the hackers pushed home their advantage, maximising the damage done by disabling the network.

With the initial phase of the attack complete, the medical provider's business was taken down with all network and telephone services offline. It was necessary to implement the Business Continuity Plan, to allow some business processes for an otherwise crippled organisation to continue. A ransomware demand in the sum of millions of dollars soon eventuated.

Due to the critical nature of the infrastructure, the first steps towards remediation were rapid initiation of a National Cybersecurity Response. Forensic work commenced, exposing the nature and extent of the breach, and ascertaining the nature of the compromised and exfiltrated information. As a notifiable breach, in addition to alerting the authorities, all affected patients were informed of the situation. Restoring the medical provider's information systems was the priority, with the rebuild of servers and endpoints taking three weeks.

From an insurance perspective, challenges included the government mandating various service providers as the affected entity is a significant national organisation. This left little control over the initial response and associated costs; despite that, the Business Continuity Plan proved effective with rudimentary systems rapidly restored.

As the insurer, Delta Insurance worked closely with the National Privacy Regulator, meeting all notification and other compliance obligations. The total sum paid out for losses incurred by the organisation amounted to nearly NZD $1 million.

A broker's perspective

As a full-time broker handling cybersecurity, I can say for sure that the landscape has changed dramatically since I entered the industry in 2019.

'Cyber risks are more prevalent than ever, with no sign of a slowdown'.

Now, change isn't always for the better or the worse. Typically, it is nuanced and that is certainly the case when it comes to cyber security and cyber insurance cover. On the positive side, New Zealand's small to medium businesses – which make up most of the commercial landscape – are increasingly aware of cyberthreats on the one hand, and the availability of cyber insurance on the other. However, this is almost certainly the inevitable result of the negative side: cyber risks are more prevalent than ever, with no sign of a slowdown. While the big hacks make the news, like the Distributed Denial of Service which hit the New Zealand Stock Exchange, or the Latitude Financial hack, or the interruption to the systems of the former Waikato District Health Board, the smaller ones hitting mom and dad shops all over the country don't.

What they do result in is discussions at the local fishing club or RSA. There are chats every day about how the local lawnmower shop got hit by ransomware, how Bob had to figure out Bitcoin, and then pay $5,000 in the hope of getting his data unlocked and systems online.

That word of mouth plays a crucial role in alerting every business owner to the uncomfortable fact that yes, their organisation is in the crosshairs of cybercriminals too. In turn, these discussions often end up with potential customers at the door of people like me.

This is where the picture becomes a little more complex. Even as the risks are up and business owners are actively seeking cyber insurance, supply from the underwriting side is down. This is for a simple reason, as outlined in the introductory note: if cyber insurance isn't done well, the risks and losses involved render it unprofitable for the underwriter. The question that begs to be answered is of course, 'What constitutes doing cyber insurance well'? In simplest terms it comes down to the foundational principles of insurance, including risk pooling, charging of premiums, and mitigating losses so the net difference between claims and premiums is a profit. If the net difference is a loss, underwriters retreat.

Cyber insurance is a relatively new kid on the block. It's why, in the insurance space, you're more likely to encounter millennials (like me) on the broking and perhaps even underwriting side, because the insurance industry veterans generally haven't dealt with the technical nature of the risk and associated controls.

'The question that begs to be answered is of course, 'What constitutes doing cyber insurance well'?'

The actuaries, too, are a bit at sixes and sevens: they like data, lots of it, and track record, and reliable projections of risks, losses and performance over the course of years, decades or longer. Cyber insurance doesn't have that history. It's also inherently unpredictable because who knows what cybercriminals might do next (sure, the same might be said for burglars – but they are generally restricted to a neighbourhood or two, while the world is literally a hacker's oyster). That said, this environment means brokers offering cyber insurance are in a better position than ever.

'Today customers looking for cyber cover come from all walks of life and every kind of industry and business'.

Customers looking for this type of cover today come from all walks of life and every kind of industry and business: growers, lawyers, and yes, the lawnmower shop. Our job is to understand the risk customers are bringing to us and sell it to the underwriters. We do this by helping clients take a business view of their risk rather than a technical view, and then coaching them on how they can establish or improve their controls to such a level that the underwriter will provide the cover they seek.

Where necessary, we will advise engaging a Managed Security Services provider or other cybersecurity expert so that a customer can achieve a cybersecurity posture suitable for their line of business, which identifies the risks they face and establishes appropriate technology and processes to mitigate those threats. Generally, we recommend not going to market until that posture is suitably robust.

Notably, there is one further aspect just as crucial in attaining good security posture, and that relates to people. Staff training and promoting awareness of cyber risks is an absolute must.

I'll end on further good news, for brokers like myself, for those seeking cyber insurance and even for the underwriters like Delta Insurance who are actively taking these risks on. Very few customers are turned away if they have put in the necessary effort demonstrating their awareness of the cyber risks they face. This, together with appropriate controls, means they are highly likely to find suitably priced cover from a specialist underwriter, even as we observe a trend of non-specialist underwriters leaving the market.

A final observation is that every business should consider going through the process of securing cyber cover. Even if you don't ultimately purchase a policy, the exercise itself will be illuminating and is highly likely to result in better cybersecurity, something which benefits the individual business and the business community as a whole.

– Jono Soo, Head of Cyber Specialty at Marsh New Zealand

The rising demand for cybersecurity in New Zealand

'The bottom line is that hackers make money when they target New Zealand.'

As far back as 2020, questions were raised about why New Zealand is a popular target for hackers.

Among the reasons are certainly universal connectivity, combined with a relatively trusting population: our physical separation from much of the world provide protection from most dangers, but fails completely in a connected world. The bottom line, though, as internet services and security provider Kordia notes, is that hackers make money when they target New Zealand[5]. This is a crucial fact for brokers and underwriters alike; it not only points to risk, but costs.

Thanks to our widespread fibre and wireless networks, New Zealand enjoys some of the best connectivity available globally. Estimates put internet penetration at 94% of the population, with InternetNZ estimating that 93% of participants use the internet daily.

While this is a snapshot of 'consumer' internet use, it is relevant to cybersecurity because consumers are also the people who work in New Zealand's industries. With estimates for the 'human element' being behind breaches put as high as 82% in Verizon's 2022 Data Breach Investigations Report,[6] people are almost always the weakest link, and that's assuming technology and process are sufficiently provisioned, appropriately configured, and hardened where necessary.

In its recent 'New Zealand's Internet insights 2021'[7] study (conducted by Colmar Brunton), InternetNZ reports that, "the number / percentage of people that are 'extremely concerned' about online privacy and security has risen for the second year in a row." The major concerns include online crime, personal data that is susceptible to compromise, identity theft and location tracking.

This is a positive development. After all, 'it isn't paranoia if they really are out to get you'. While the information security industry is often pilloried for its use of 'fear, uncertainty and doubt', every internet user should have a healthy level of awareness of the reality of these risks every time they use a computer or smartphone.

'Estimates put internet penetration at 94% of the population, with InternetNZ estimating that 93% of participants use the internet daily'.

A less positive development is associated with escalating cybersecurity breaches. A November 2022 report in the New Zealand Herald[8] notes that while the total number of incidents remains fairly static, the number of 'successful' attacks has increased substantially. The report quotes CERT NZ, saying "...the number of attacks resulting in loss through fraudulent criminal activity and unauthorised access to victims' accounts has jumped by about 30 per cent" and with direct losses of nearly $9 million in just three months. Research cited in a Newshub report put the average cost of a cyber breach to a New Zealand business at $159,000[9].

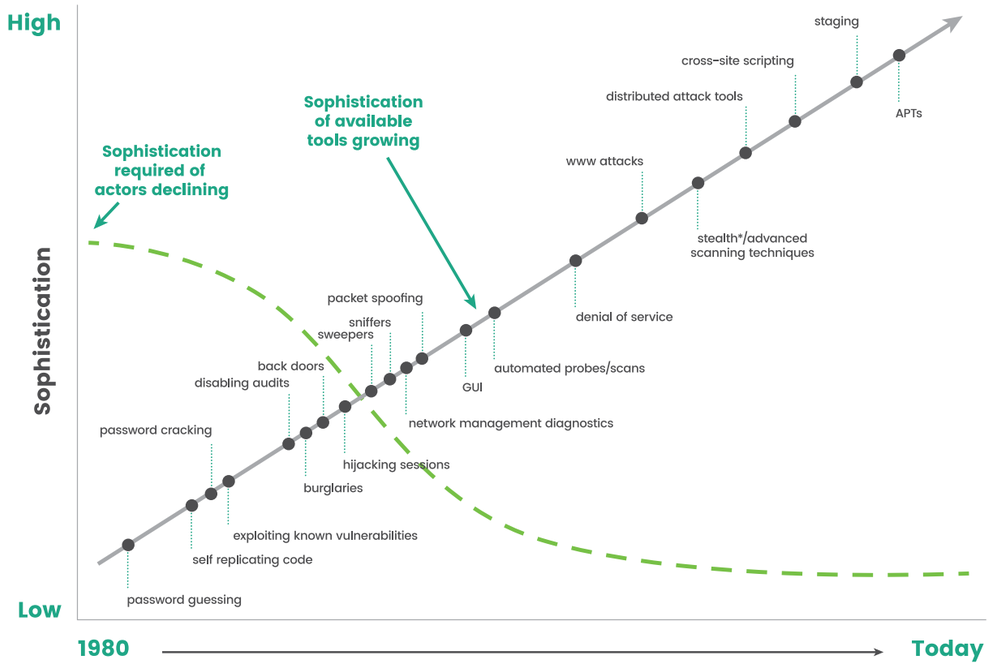
The full cost may be higher, as the Actuaries Institute of Australia[10] estimates the cost of cybercrime to the Australian economy at $33 billion for the last financial year, while the global average cost of a data breach is $4.35 million.[11]

Facing losses of this magnitude, demand for cybersecurity insurance is increasing significantly as organisations of all types and sizes appreciate the magnitude of the risk. Along with business liability, cyber is becoming an essential service, because without protection a single breach could cause organisational failure. With demand increasing, look for more availability of cybersecurity insurance. This also means more policy options, which is good for those seeking coverage.

The impact on businesses and establishments of national significance is substantial. The National Cyber Security Centre Cyber Threat Report 2021/2022[12] recorded 350 cyber incidents while successfully disrupting over 122,000 incidents. Recent high profile attacks include the New Zealand Stock Exchange, Waikato DHB and Mercury IT, which demonstrated supply chain risk and the affect on multiple government agencies and businesses that used the service provider's services[13]. In 2021, research from accounting software firm MYOB[14] showed a quarter of New Zealand's small to medium businesses suffered a ransomware attack.

Aside from financial loss from theft or extortion, the impact of a cyberattack can also include disruption to business processes, reputational damage and remediation costs. While prevention is always better than the cure, it is an uncomfortable reality that even the prepared, cyber-aware and most secure organisation can fall victim to an attack.

Cyber crime historical overview



Types of attacks and their perpetrators

The barrier to entry for cybercriminals is low. Perpetrators range from mischief-making teenagers through to sophisticated, well-organised and well-funded criminal groups structured and operating like a business.
Even entire nations are targeted with state-sanctioned attacks as part of espionage or cyber-warfare initiatives (though this falls outside the scope of this white paper).

The tools used by cybercriminals are readily available on the 'dark web', as is support, encouragement and assistance from similarly minded criminals acting in concert online.
A recent news article showed that prospective hackers can set themselves up with the necessary software and techniques for as little as a few hundred dollars[15].

This is confirmed in the Sophos 2023 Threat Report[16], which concludes that there has been "...the continuous lowering of barriers to entry for would-be cybercriminals and the commodification of what once would have been considered "advanced persistent threat" tools and tactics. While there has long been a thriving marketplace for hacking tools, malware and access to vulnerable networks, the lessons learned from the recent history of ransomware operations and other well-funded malicious actors are more rapidly becoming available to the wider criminal community—as are commercial security tools designed to defeat some defenses..."

The methods, techniques, tools, and tactics used by cybercriminals are numerous, ever-expanding and constantly evolving. TechTarget[17] lists at least 13 types of attack. Knowing what these attacks are and how they work is highly recommended for every broker. Recognising and understanding cybercrime attack methods helps identify and avoid becoming a victim and informs a risk management mindset.

'A recent news article showed that prospective hackers can set themselves up with the necessary software and techniques for as little as a few hundred dollars[15].

As new tools emerge, hackers often adopt them faster than commercial organisations can, because the 'product development' lifecycle for those operating outside the law is not restricted by quality control, health and safety, and other legalities. Hackers and information security professionals have long engaged in an 'arms race', each seeking the advantage of a new technology or technique before the other can. The emergence of artificial intelligence is being put to use by both sides[18]. While 'ethical programming' sets out to limit its express use for nefarious purposes, platforms like ChatGPT are likely being used by hackers to accelerate malware development.

The different types of cyber attacks include malware (and ransomware); methods targeting passwords and identity (to gain unauthorised access); Distributed Denial of Service (to interrupt crucial services); phishing; targeting of databases (such as SQL injection); cross-site scripting (which compromises websites); man-in-the-middle attacks (intercepting messages between two parties); DNS spoofing (fooling people to visit fake sites); botnets; watering hole attacks; and insider threats.

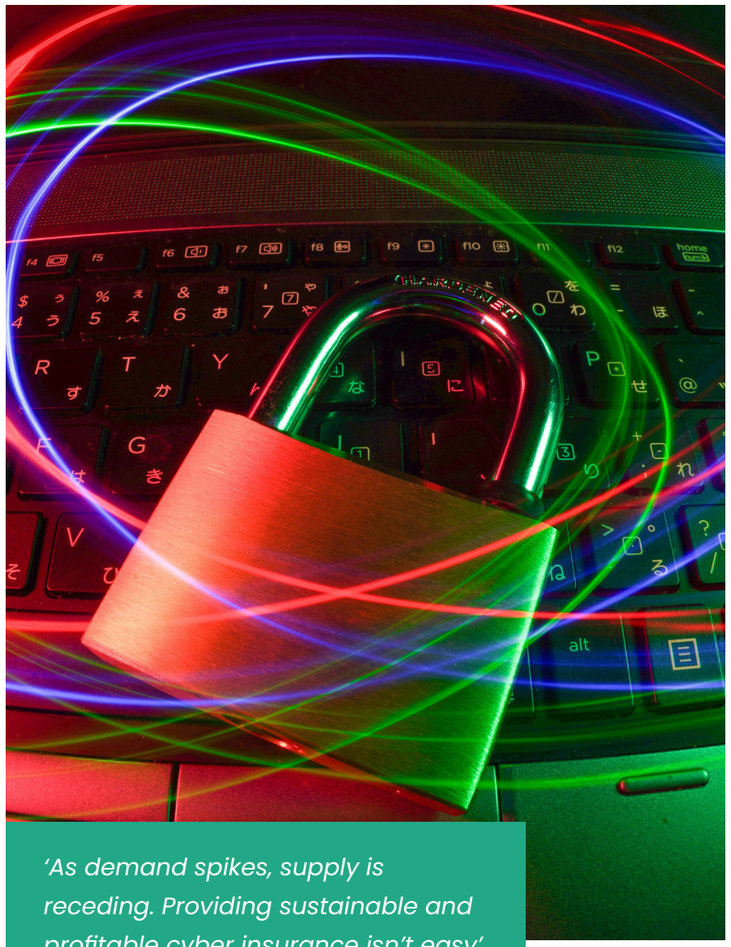
These methods are often used combined, with the goal of extracting valuable information (often usernames and passwords, or banking PIN numbers) for later use to extract money or extract more information for use as a ransom.

Multiple reports from security technology vendors, government organisations and research companies confirm an escalating threat environment along with rising costs for effective protection. The Kaspersky Security Economics Report[19] quantifies the costs, with the following key findings:

- Cybersecurity budgets in 2022 averaged $3.75m for enterprises and $150k for SMEs. Both segments are planning to increase budgets equally up to 14% in the coming year.
- Communications, product development and customer support are the top three processes most affected by cybersecurity intrusions.
- Data leaks were the most encountered security issue this year, most often caused by employees (22%) and attackers (23%).
- Delivering cybersecurity solutions and efficiencies by bringing in external experts are the main drivers leading companies to outsource IT security.

In short, cybersecurity risks and costs are real and substantial. Providing cyber insurance cover sustainably therefore depends on a cautious, risk-management approach where underwriter, broker and customer work together towards the common goal of quantifying and mitigating cyber risk, with insurance one component in a broader cyber resilience strategy. The Actuaries Institute of Australia[20] notes, 'while the first line of defence against cyber risk will always be good cyber hygiene and security, cyber insurance is an important second line of defence.'

Demand for cyber insurance increases as supply recedes



'As demand spikes, supply is receding. Providing sustainable and profitable cyber insurance isn't easy'.

Given the significant threats and losses in the event of a hack, demand for cyber insurance is increasing substantially in New Zealand and around the world.

There is also increased awareness of the availability of insurance protection against cyber threats. However, even as demand spikes, supply is receding. Providing sustainable and profitable cyber insurance isn't easy and depends on appropriate knowledge and insight into the complex world of information technology as well as business.

A Fortune Business Insights paper[21] anticipates growth in the global cyber insurance market at a CAGR of 25.7% between 2022-2029, increasing from US$12.83 billion to US$63.62 billion. The paper notes increasing incidences of hacking along with the risks of fines and other punitive measures from governments for customer data breaches. It also points to the reality of small and medium businesses coming into the crosshairs of attackers.

'While the first such products emerged in the 1990s, the appeal of and necessity for cyber insurance has escalated in recent times'.

Research and Markets[22] offers a slightly less rosy forecast and assesses the value of the global market considerably lower, at US$7.06 billion in 2020. It anticipates growth at a CAGR to US$20.43 billion in 2027.

Despite the differing views, what is clear is that cyber insurance is a potentially lucrative market. While the first such products emerged in the 1990s, the appeal of and necessity for cyber insurance has escalated in recent times (and indeed it has escalated dramatically since Delta Insurance entered the market in 2014).

However, many insurers are realising that the rich market value and double-digit growth figures are far from easy money. The utmost care is required in providing cyber insurance. As payouts increase, supply is dwindling, coverage terms are becoming more restrictive, and premiums are escalating. Careful insurers running a profitable book, it should be noted, are less likely to increase their premiums, though these premiums were likely comparably high in the first instance, reflecting the substantial due diligence invested into every policy. In fact, an April 2022 Fitch Ratings report found that cyber premiums rose by 74% in 2021.

With the increase in cyberattacks has come an increase in insurance payouts. Insurance companies are increasing premiums to keep up. A more recent CNBC report[23] confirms that rising premiums along with reduced supply may make cyber insurance unaffordable for some companies.

In New Zealand, the situation mirrors that in the rest of the world. Cyber breaches are increasingly common. It isn't just the high-profile ones which make the news, but many smaller hacks are also affecting small local businesses. These incidents don't appear on the Morning Report bulletin, but they are discussed at the local Chartered Clubs. Awareness is heightened, most people know someone who has been hit, or may even be a victim of ransomware or other hacks themselves.

At the same time, demand is up and the insurer's risk appetite is reducing. General insurers are showing increasing caution, as the costs of providing effective cover to the mass market aren't economical, causing a 'flight to specialisation'. Some coverage is more difficult to find, and it is harder for local businesses to secure cyber insurance. In other areas, such as state-sponsored cyberattacks, coverage is being withdrawn altogether. Starting in 2023, Lloyd's of London Ltd. requires exclusion of catastrophic state-backed hacks from standalone cyber insurance policies[24].

In providing cover, complete assessments of the cyber security posture of the client is necessary before writing any policy. Controls typically assessed by brokers and underwriters include:

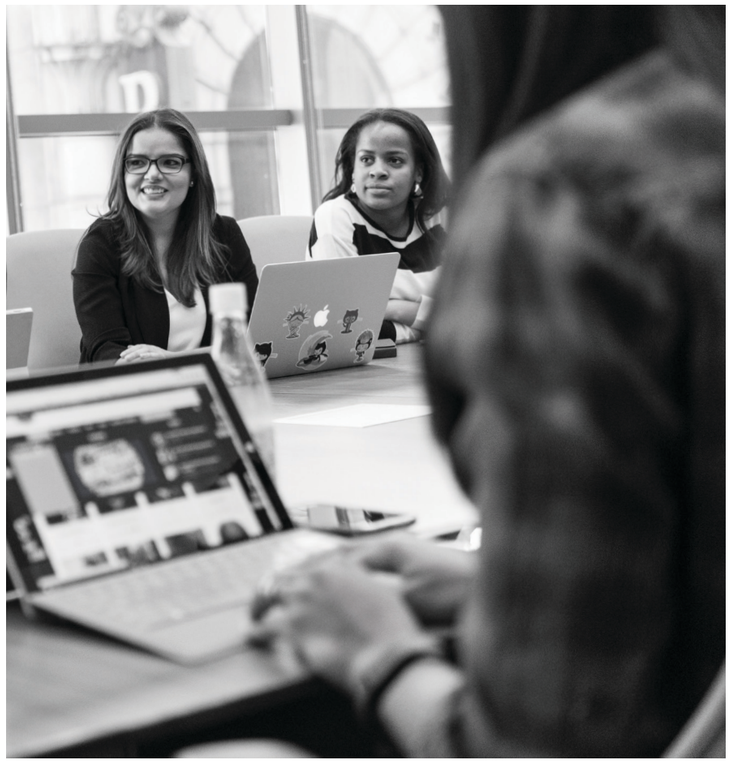
- Multifactor authentication for remote access and admin/ privileged access
- Endpoint Detection and Response (EDR)
- Secured, encrypted, and tested backups
- Privileged Access Management (PAM)
- Email filtering and web security
- Patch and vulnerability management
- Cyber incident response planning and testing
- Cybersecurity awareness training and phishing testing
- Hardening techniques including Remote Desktop Protocol (RDP) mitigation
- Logging and monitoring/network protections
- End-of-life systems replaced or protected
- Vendor/digital supply chain risk management

Cybersecurity posture will impact cover

Leading local law firm MinterEllisonRuddWatts notes in an online paper[25] that securing cyber insurance is getting harder, with the following assessment:

"Insurers are responding to the rising risks and costs of cyber events with increasingly detailed assessments of insureds' IT systems, while in some cases also reducing cover limits and increasing premiums. Others have reduced limits significantly or withdrawn cover altogether. Large firms, such as those with revenue over NZD$100 million, are facing particular scrutiny, as they present an increased perceived risk as more attractive targets to criminals".

The law firm further advised, "The complexity of insurers' questionnaires and their importance means that IT departments must be well prepared and resourced to answer them. This should be done well in advance of the cyber insurance renewal date, as the time commitment is significant, and answers often need to be drawn from different sources. IT departments may realise as they work through the questions that the answers they would give will not satisfy insurers, so it may be necessary to take remedial steps urgently so that a more satisfactory response can be given".



Any business seeking cyber cover is well-advised to consult with an IT provider with proven cybersecurity capabilities ahead of or in conjunction with the insurer. The process of testing the market for cover can itself contribute to an improved security posture, as cover will only be extended if risks are suitably quantified and appropriately mitigated through demonstrable plans, measures, processes, technology and personnel.

"While cyber insurance is increasingly challenging to obtain, brokers report that it continues to benefit insureds. They report that, perhaps because of the care taken when it is arranged, it features a relatively high claim acceptance rate compared with other types of insurance, so notwithstanding the cost and time investment required, it is worthwhile and provides a real benefit. "Cyber insurance also remains one of the few insurance products that assists insureds to prevent claims. Insurance assessments are often valuable tools to identify security weaknesses and remedy them, as insurers often have up to date knowledge of the latest risks.

Cyber insurance discussions can therefore benefit insureds by assisting them to improve their systems and remove vulnerabilities. Cyber insurance provides a badge of quality, as it demonstrates that an insurer has assessed the insured as a good risk."

'The barrier to entry for new cybercriminals is low, while their reward potential is high'.

A lucrative market for specialists

It is clear from multiple threat reports that the cyber risk environment for all business types is escalating.

Cybercriminals operate somewhat indiscriminately from the safety of geographically distant locations, often with little or no fear of consequences from law enforcement.

Their organisations and activities are profitable, adding impetus and emboldening their activities. The barrier to entry for new cybercriminals is low, while their reward potential is high, further heightening the threat environment for every legitimate business. Meanwhile, New Zealand's trusting population and universal reliance on connectivity for commerce make it an enticing target.

Providing cyber insurance isn't a fast, simple transaction. Instead, it rests on considerable expertise, has a long sales cycle, and requires brokers to work closely with customers and underwriters.

However, there are long term benefits for the brokers who choose to specialise and work with an increasingly circumspect group of cyber underwriters which have the necessary knowledge, experience and track record in delivering sustainable solutions. What is clear is that caution is advisable for both brokers and underwriters, who must accurately assess and gauge risk before writing policies. By the same token, organisations seeking cyber security cover are well-advised to seek the advice and guidance of their IT providers and cyber security specialists.

While capacity is retreating and is likely to continue doing so, New Zealand's business owners are still well positioned to secure cybersecurity cover. However, this is only possible for those organisations demonstrating an appropriately rigorous, proactive and comprehensive approach to risk mitigation.

As generalist brokers find cyber insurance risk unpalatable, a flight to quality is advised, as is acting sooner rather than later to secure cover while improving the overall cyber risk posture.

About Delta Insurance

Delta was established in 2014 to answer the call for insurance in new or specialised areas, with exceptional customer service - all underpinned by transparency and integrity.

Today we cover over 30,000 risks in New Zealand, Singapore and Australia. We are proud to have won ANZIIF's Insurance Underwriting Agency of the Year award in New Zealand for the last five years for our continued focus on our customers. As well as resolving claims, we focus on prevention using a range of risk mitigation strategies, partnerships and solutions.

delta

Our Philosophy

Our Vision
We embrace change to make the world a safer place.

Our Mission
We give you the confidence and security to succeed.

Our Values
With our entrepreneurial spirit, we're proactive and nimble.
We do the right thing. We're passionately curious.
We're at our inspirational best when we collaborate.
We enjoy the journey and celebrate it.

Sources

1 https://www.nzherald.co.nz/nz/scammers-siphon-millions-from-kiwi-victims-in-elaborate-cyber-attacks/NY6THLPNUJDHRO6VC6WSEJJAIE/

2 https://www.theguardian.com/world/2020/sep/01/new-zealand-stock-exchange-hacks-who-is-behind-them-and-why-now-explainer

3 https://en.wikipedia.org/wiki/Waikato_District_Health_Board_ransomware_attack

4 https://www.cshub.com/attacks/news/new-zealand-government-compromised-in-third-party-cyber-attack

5 https://www.kordia.co.nz/news-and-views/cybercrime-pays-off-when-new-zealand-businesses-are-targeted

6 https://www.verizon.com/business/resources/reports/dbir/

7 https://internetnz.nz/new-zealands-internet-insights/new-zealands-internet-insights-2021/

8 https://www.nzherald.co.nz/nz/scammers-siphon-millions-from-kiwi-victims-in-elaborate-cyber-attacks/NY6THLPNUJDHRO6VC6WSEJJAIE/

9 https://www.newshub.co.nz/home/technology/2021/10/cyberattacks-on-new-zealand-businesses-increasing-dramatically-now-cost-an-average-of-159k-each-research.html

10 https://actuaries.asn.au/public-policy-and-media/thought-leadership/green-papers/cyber-risk-and-the-role-of-insurance

11 https://www.ibm.com/reports/data-breach

12 https://www.ncsc.govt.nz/assets/NCSC-Documents/2021-2022-NCSC-Cyber-Threat-Report.pdf

13 https://www.bankinfosecurity.com/ransomware-attack-in-new-zealand-has-cascading-effects-a-20636

14 https://www.myob.com/nz/about/news/2021/nearly-a-quarter-of-smes-in-new-zealand-victims-of-cyber-attacks

15 https://www.stuff.co.nz/business/129543714/the-dark-web-where-you-can-destroy-a-business-for-300

16 https://www.sophos.com/en-us/content/security-threat-report

17 https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them

18 https://www.techopedia.com/ai-in-cybersecurity-the-future-of-hacking-is-here/2/34520

19 https://calculator.kaspersky.com/

20 https://actuaries.asn.au/public-policy-and-media/thought-leadership/green-papers/cyber-risk-and-the-role-of-insurance

21 https://www.fortunebusinessinsights.com/cyber-insurance-market-106287

22 https://www.researchandmarkets.com/reports/5636783/global-cyber-insurance-market-forecasts-from

23 https://www.cnbc.com/2022/10/11/companies-are-finding-it-harder-to-get-cyber-insurance-.html

24 https://www.wsj.com/articles/lloyds-to-exclude-catastrophic-nation-backed-cyberattacks-from-insurance-coverage-11660861586

25 https://www.minterellison.co.nz/insights/cyber-risk-and-cyber-insurance-themes-and-predictions