ISSUE 3 FEBRUARY 2017

New technologies bring new risks

Embracing Technology Risk Management

Thought Leadership Series

DELTA™ INSURANCE

CONTENTS

Embracing Technology Risk Management

As New Zealand's third largest export behind dairy and tourism, the technology sector stands as one of the most vibrant and promising components of the New Zealand economy. In addition to creating value and thousands of jobs, the local technology sector epitomises Kiwi ingenuity and entrepreneurial flair.

With exports amounting to nearly $7 billion and total revenue predicted to exceed $10 billion in 2017[1], the technology industry is carving out its own niche on the global stage, as well as shaping up to be an integral part of the New Zealand economy.

Yet in an increasingly globalised world, an industry which often relies on multi-regional interconnectivity faces a host of potential problems that can endanger businesses both large and small. Technology-specific issues enhance the scope of risk technology businesses face, due to a greater level of liability stemming from technology operations. The highly litigious nature of the North American and European markets is gradually becoming a global phenomenon, with its influence felt ever-increasingly in Australia and New Zealand, thus widening the net of legal liability that can ensnare technology business, particularly in the field of intellectual property law. In addition to the enhanced risk associated with intellectual property, the reliance on third party vendors leaves many businesses prone to liability risks (such as third party service failure and service outages) that they may be unprepared for.

We believe it is paramount for all technology businesses, whether they are in their infancy or embarking on global expansion to be aware of the risks associated with being a technology company, as well as understanding the risk management options available.

This paper aims to guide and assist New Zealand technology businesses in managing and understanding the risks they face in providing their technology services and how insurance can be used as part of a comprehensive risk management strategy to lessen their exposure to technology liability risks.

Snapshot of the Technology Industry

The New Zealand technology industry stands as one of the bright spots in what's already seen as a 'rock star' economy. With local innovators such as Xero and Orion leading the charge on the global stage, the New Zealand technology industry has developed an international reputation for innovation and entrepreneurship. The fastest growing sector in New Zealand, technology exports have doubled in the last decade[2], with some even predicting it to eventually overtake the dairy industry.

In addition to providing value within the local market, the biggest factor of the technology industry is its foreign market viability. Technology is New Zealand's third largest export industry, with exports doubling between 2008 and 2014[3] and the Technology Industry Analysis Report 2016 (TIN 100) crediting overseas markets for contributing to over 80% of growth in TIN companies in 2016.

High-tech manufacturing

While comprising a lower workforce, the high-tech manufacturing sub-sector is credited with higher revenue growth and export value. The value of the industry – featuring subsectors such as pharmaceuticals and scientific equipment manufacturing - to the New Zealand IT industry as a whole is highlighted by high-tech manufacturing generating 61% of the total revenue earned by TIN companies in 2016. It remains an export-reliant component of the tech industry that provides the greatest value offshore - over 80% of its revenue is earned outside New Zealand, with the USA and Australia comprising nearly half of its total market[4].

ICT sector

The ICT sector has been credited with contributing nearly $20 billion to the New Zealand economy[5], and is responsible for a fifth of the total New Zealand workforce[6]. The ICT sector – comprised of telecommunications, computer system design, IT services, IT manufacturing and IT wholesaling - has quickly forged an image in the local and global market as a beacon of Kiwi entrepreneurship and ingenuity. With cloud computing becoming increasingly ubiquitous in business operations, the demand for such services will continue to increase, both here and abroad.

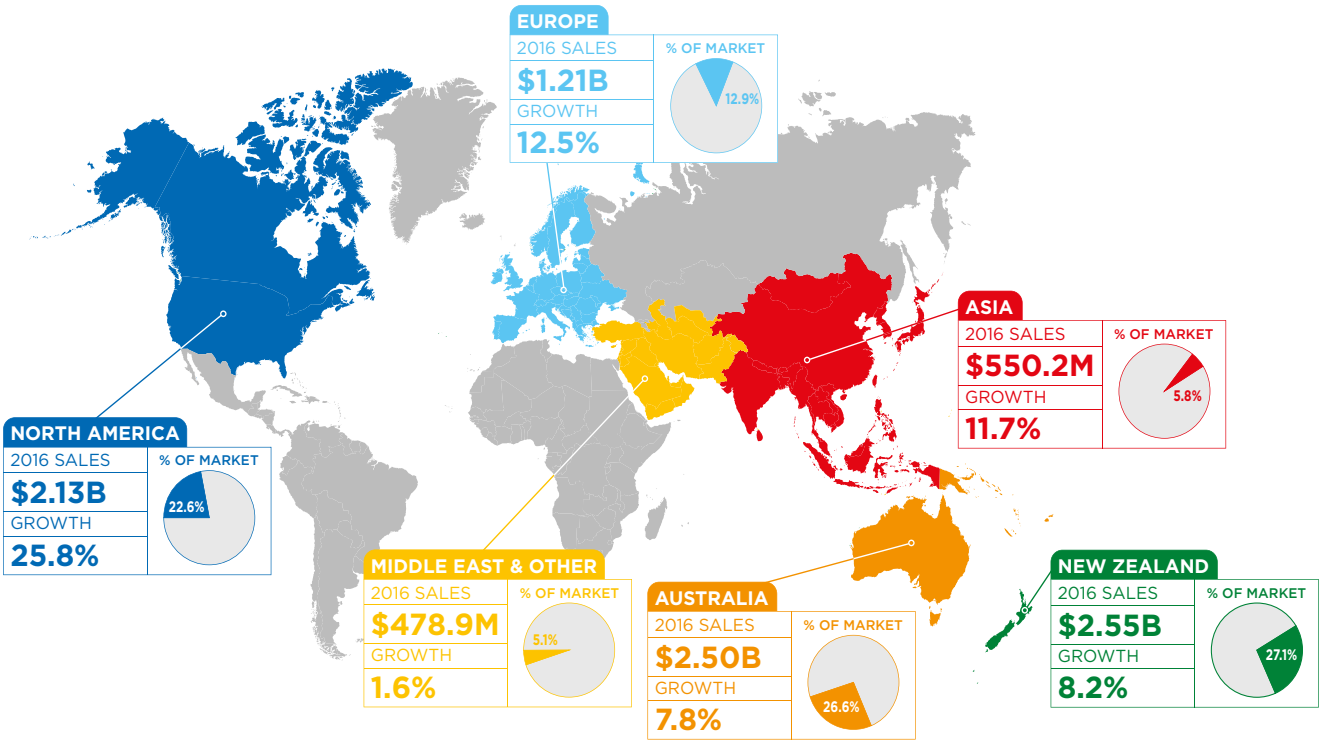
The Local Market

All regions in New Zealand experienced growth in the IT sector in 2016, with Wellington seeing the highest revenue growth of 15.3%. Wellington is increasingly becoming a hub for IT businesses, hosting local giants such as Xero and TradeMe, and experiencing an increase in IT infrastructure. Outside Auckland and Wellington, both the South Island and Hamilton have seen substantial growth in revenue, indicative of a nationwide boom.

Unlike construction, agriculture and other industries, where substantial start-up capital costs are often involved, technology businesses often require nothing more than a good idea and a laptop in order to get things rolling. Add to this a supportive government, industry advocates and educators (such as NZTech), along with few internal constraints on expansion both in New Zealand and overseas, it's likely that the results that we have seen in the past will continue for years to come.

The International Market

Perhaps the greatest source of encouragement for New Zealand technology businesses is the successes of local companies in North America. In addition to rapid increases in IT exports to North America, the success of local companies has seen an influx of foreign investment in New Zealand IT businesses, with an estimated quarter of leading American venture capital and private equity firms holding investments in New Zealand IT businesses[7].



Sales, Annual Growth and Percentage Share of key markets for Top 200 TIN Companies in 2016

The European market has also witnessed a sustained increase in tech exports over the past few years, partially aided by the fall in the value of the euro. The development of local high-tech manufacturing has the potential to reap significant dividends in the future, when considering the prospects of potential trade deals with the European Union and the United Kingdom. New Zealand companies such as Datacom and Powershop have already made the successful jump into the European market. Yet the prospects for expansion don't just apply to larger companies: smaller firms have also started to look to Europe as a key market to export high-value offerings[9].

New Zealand businesses have also started to embrace Asia as a potentially lucrative market for technology exports. With its enormous population, burgeoning economies and a massive labour force, the Asian market offers well-established New Zealand companies the opportunity to carve out their own niche. The desire to tap into the Asian market has been highlighted through ventures like the expansion into Vietnam by Augen, Xero into Singapore[10], and Datacom's expansion into the Philippines. The prospect of comprehensive trade deals with viable markets like Japan and ASEAN offer further incentives for enterprising technology companies to expand in the years to come.

However, technology companies must also be aware that with expansion into foreign markets risk management strategies and procedures may also need review. With the greater potential revenue to be realised in viable markets such as the USA and Europe comes a far greater risk of legal liability. The stringent intellectual property laws in the USA and a far more litigious and highly regulated environment create new and greater liability risks for technology businesses which they have to prepare for should they seek to reap sustainable rewards in the US market. It's also important to note that such attitudes are not isolated to one market – they are in fact, indicative of a growing global trend towards heightened litigiousness.

With the greater potential revenue to be realised in foreign markets comes a far greater risk of legal liability

Major Risks Technology Firms Face

Whilst the risks technology firms face are broad and often global in nature there are certain areas of risk that are common to the majority of technology companies, regardless of their size, global footprint or the technology services they provide. This next section seeks to expand and provide commentary on some of the common areas of risk faced by technology companies.

Scope Creep

Scope creep stands as a near-universal problem in an industry well known for delivering bespoke services and projects. A common risk in IT project management, scope creep arises when the scope of a project expands beyond what was previously anticipated, and bloats into something unattainable. The majority of technology liability claims witnessed by insurers both in New Zealand and overseas involve scope creep and project failure-related issues. Scope creep is characterised by three main failures: failure to deliver on time, failure to meet the budget (with an estimated 85% of projects ending up over-budgeted to some degree[11]), and a failure to meet customer expectations. Scope creep can occur due to many reasons:

The majority of technology liability claims witnessed by insurers both in New Zealand and overseas involve scope creep and project failure-related issues

- Adding previously unplanned features in the hopes of enhancing the project's value
- Scoping the project incorrectly
- Making unplanned alterations
- Underestimating the project's complexity
- Misjudging the requirements

Scope creep is a ubiquitous problem across all countries, and New Zealand is certainly no exception. New Zealand companies have been burned in the past due to scope creep, with some even being forced into liquidation after struggling to manage lucrative projects with an ever-expanding scope[12]. It is not unusual to see technology firms feel pressured into widening the scope of their projects beyond their reasonable capability in the hopes of maintaining high-value contracts.

Project managers should also aim to avoid the process of gold-plating, where customers are given more than what was originally planned[13]. Should scope creep inevitably occur midway through the project, it's ideal for all parties involved to have back-to-back contracts at the start of the project, with the nature and terms of the contracts being similar across all parties. This can limit the liability imposed on contractors and subcontractors[14] [15].

Intellectual Property Liability

With overseas expansion comes the greater likelihood of intellectual property (IP) infringement. Operating in a multi-national capacity can leave you prone to IP infringement action due to the larger pool of innovation and patents whose rights you might find yourself unknowingly infringing. Different countries have different IP protection rules, which complicates matters when working in a multi-region capacity, particularly when some jurisdictions are more stringent than others. The level of intellectual property litigation in the USA and Europe exceeds what we see in New Zealand, with similar attitudes arising among Asian regulators in recent years[16] [17]. It's clear that for New Zealand technology firms to thrive in overseas markets, they must be able to withstand the rigours of stringent IP regulation.

Patent Issues

Although software patents are not recognised in New Zealand, the same unfortunately does not apply for other jurisdictions. The debate concerning exactly what is patentable varies across countries, and remains a contentious issue among legislators. For example, while not banning software patents outright, Australia has limited restrictions on the patentability of software. Software patents have been granted in the USA since the 1970s, and there is increased concern that the proposed Unified Patent Court will allow the patentability of software in the EU. Outside North America and Europe, Asia is quickly becoming the fastest growing region in terms of patents filed[18], largely driven by the advances made in the technology sector and the escalation of the Smartphone Wars.

New Zealand technology companies have suffered in patent infringement cases brought by multinational companies in recent years. A New Zealand technology company which develops noise cancelling software, was forced to settle with US audio giant Bose over a claim of patent infringement. The New Zealand company was alleged to have created headphones for third parties that infringed on some of Bose's patents. Despite offering no admission of infringement or liability, the New Zealand technology company was regardless forced to settle. The third parties that manufactured the headphones for the New Zealand company were also required to individually settle with Bose[19]. This case emphasises the disparity in bargaining power held by small

Open Invention Network

The Open Invention Network (OIN) is the largest non-aggression patent pact in the world designed to protect and enable the use of Linux. It is comprised of members, associates and licensees, and aims to share open source software information while circumventing potential legal action for patent infringements. OIN aims to curb patent lawsuits by acquiring patents and licensing them royalty free to its network partners. The partners reciprocally agree not to assert their own patents against Linux and Linux-related systems and applications. It was founded as a response to the growing number of software patent litigation. Its members include tech giants like Google and IBM, and holds over 2100 licensees as of 2016[21].

Kiwi companies aiming to compete in a market of giants. Due to the high legal costs arising from intellectual property disputes that can't realistically be shouldered by many aspiring smaller businesses, smaller players in the market can find themselves being bullied into settling regardless of their level of culpability. This also subsequently tarnishes a company's public image and can have a significant long-term impact on their viability in the marketplace. What's also of concern is that the primary defendant is not the only one at risk – as illustrated above, secondary parties associated with the defendant may also face liability, thus risking getting dragged into expensive settlements.

Patent Trolls

Patent trolls often purchase patents from bankrupt companies or entities unable to afford patent rights, and aim to create income by targeting businesses for patent infringement. Such alleged infringements can arise from using the troll's patented work in their own products, or even simply using the patented work through the course of their operations.

Some notable cases of patent trolls and patent infringement:

1. New Zealand technology company Zeacom was hit twice by patent trolls in North America. The first where defending the allegation would have cost in excess of US$1,000,000 was settled for $350,000. The same troll was said to hit 85 businesses on the same day, with nearly all of them paying up[20].
2. One of the more extreme cases of patent troll claims saw Blackberry Limited reached a settlement with a patent troll for a colossal US$612.5 million in a claim over patent infringement[22].
3. Patent trolls have also been known to patent business ideas. In 2012, several major companies such as Apple and McDonald's were hit by a patent troll's claim alleging infringement over the use of sending website links in promotional text messaging. While most companies complied with the troll's demand for a payment of $750,000, The New York Times and other companies led a legal battle against the patent troll[23], which they subsequently lost in 2015[24].

The risks of encountering patent trolls vary from jurisdiction to jurisdiction, with a greater frequency of incidents occurring in the USA where the regulatory regime remains more litigious than other markets, such as the United Kingdom. The 'loser-pays' standard of the UK courts dissuades trolls from commencing litigation to the extent that is seen in the USA.

> Patents are a big, big nasty area and local companies by and large have no idea how it works. As soon as you get your head above the parapet you've got a problem because there are all these trolls going around in every industry just waiting to see who they can have a go at
>
> *Miles Valentine, Zeacom founder*[21]

The further you expand in a foreign market, the more attention you're likely to draw from serial litigants and patent trolls. Thus, the opportunities to incur greater revenues and market presence overseas brings with it its own risks. It's recommended to search the patent register of the country you plan on expanding into and check for any established patents which your products might infringe. Legal advice on intellectual property prior to commencing business in new regions is also highly recommended.

Copyright Issues

Intellectual property issues are not restricted to patents alone. The contentious issue of incorporating copyrighted source code into software requires careful consideration. There have been numerous cases where technology contractors have found themselves on the receiving end of a claim based on copyright infringement. As it stands, the source and binary code in software is defined as a "literary work" and is thus treated as copyrightable under New Zealand law. Copyrights generally have internationally recognised standards, putting companies at high risk of unwitting copyright infringement. By incorporating copyrighted material into your products and services, you can find yourself unintentionally infringing the copyright of a patron in another country, even if you aren't operating in that country, due to international copyright agreements.

Here are some scenarios where you might find yourself liable for copyright and trademark infringement:

- A Software-as-a-Service (SaaS) provider is accused of copyright infringement by a competitor who claims that their copyright has been infringed through the incorporation of copyrighted source code by the SaaS provider without permission.
- An animation studio creates informational videos for a university's website. They include music in the background, which happens to be copyrighted. As they are using the music without the author's permission, they can be found liable for copyright infringement.
- A website developer creates a website for an online retailer. However, a widely-known rival retailer already has an established website with the same colour scheme, features and page design and sees the website as attempting to pass itself off as its larger rival. The first online retailer is subsequently accused of infringing its rival's trademark and likeness, and looks to the website developer for compensation. The website developer is subsequently forced to re-design the website from scratch, incurring extensive costs.
- A software game developer creates a rugby game that features the photo of a top rugby star on the cover. The developer has sought the permission of the photographer, but not the permission of the player to use his likeness. The developer is later sued by the player for using his image and likeness without permission.

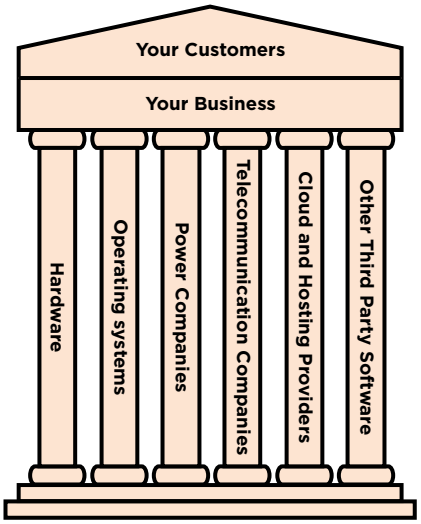
Reliance on third party vendors

In order for technology companies to provide their products and services to their customers, they are reliant on other parties to help them facilitate this process. If raw materials are not supplied to a manufacturer, or they suffer a power outage, they are unable to produce their product. Similarly, technology companies are often reliant on third party providers such as cloud service providers and ISPs, where their failure can result in the inability to provide your service. There is also a heavy reliance on physical hardware, power supply, firewalls and malware-detecting software, right down to your operating system.

No operating system or software is fool-proof. For example, Windows released a patch in August 2016 to fix 27 known bugs, some of which included fixes for critical security and operational vulnerabilities. Oracle's first security patch for 2017 contained fixes for 270 vulnerabilities, mostly in the business-critical applications. Any one of these vulnerabilities if not patched could be exploited by hackers and interrupt your business operations, leaving you unable to provide technological services and products to your customers. The increasing popularity of apps can also create additional exposure for a business if any vulnerabilities exist within such apps. In the past 2 years, Google has pressured app developers to patch security issues in more than 275,000 Android apps hosted on its official app store.

Reliance on these third parties to provide essential services such as cloud computing, software development and telecommunications, creates a particular risk for companies who supply continuous services to their customers. A failure of a service provider impairs your ability to provide your technology services through no fault of your own. These failures or interruptions of services to you can result in your customers looking to hold you liable for costs they incur. Several businesses both large and small saw their systems left offline after the cloud provider Amazon Web Services (AWS) was affected after bad weather inflicted hardware damage to one of Amazon's data centres[25]. Likewise, an outage suffered by UK-based SaaS platform provider SSP caused significant business interruption to several New Zealand insurance brokers for three weeks leaving many unable to conduct any business operations[26] and some considering seeking compensation[27].

Failures of offshore service providers can thus have widespread implications to your business. If you accept liability for not providing your technological services to your customers, you may incur substantial costs that could have been prevented had you limited your liability by accounting for the factors specified above.



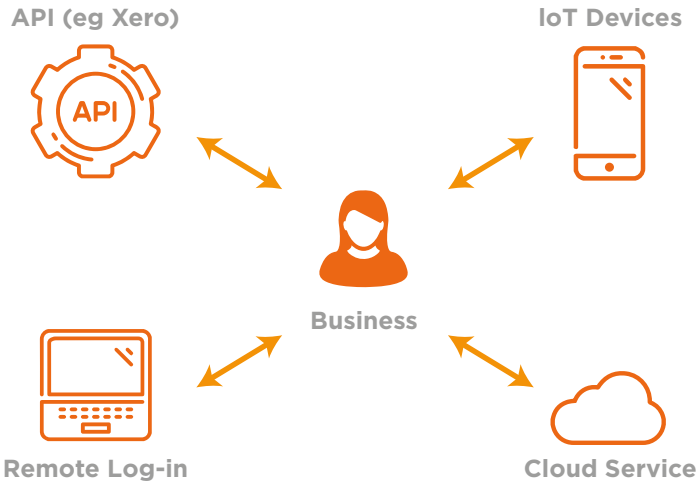
Reliance on these third parties to provide essential services creates a particular risk for companies who supply continuous services to their customers

British Sky Broadcasting Group vs Electronic Data Systems

When tendering for projects, there is the temptation to promise more than what can realistically be delivered. The most notable instance of this was the BSkyB vs EDS case. EDS was tasked with developing and integrating a CRM system for BSkyB's subsidiary. The original project was budgeted at £50m, and forecast to last for 27 months. However, the project subsequently went awry, incurring significant costs and only reaching completion 6 years later. BSkyB filed action against EDS for a number of charges including fraudulent misrepresentation, and alleged damages of £709 million

What's particularly striking about this case is that although EDS' contract stated a liability limit of £30 million, this proved ineffective as liability cannot be limited by contract in cases of fraud[29]. The eventual settlement exceeded the contractual limit of liability several times, culminating in a final settlement of £318 million[30]. The misconduct committed by EDS' sales representatives also offers a valuable lesson to technology companies to closely monitor all facets of their business operations. Technical staff may find themselves let down by the actions of sales representatives, and vice versa.

Although EDS' contract stated a liability limit of £30 million, this proved ineffective as liability cannot be limited by contract in cases of fraud[29]. The eventual settlement culminated in a final settlement of £318 million[30]



Increased interconnectivity of your business increases your business risk

Errors & Omissions

Even with robust defect management strategies in place around software development and implementation, errors can still arise. Whether it be simple errors in coding (that may not have appeared in a test environment, but once the system goes live became visible), errors in specification or design or just misunderstanding the scope required in the tendering process, all of these errors can have serious ramifications.

In certain instances incorrect scoping of a project has been viewed as outright fraud and dishonesty, rather than being seen as a simple error or omission. This can arise where overzealous sales representatives make fraudulent misrepresentations in relation to the availability of resources, time, cost and the viability of the software[28] [29]. Errors and omission risk can be mitigated by having appropriate peer review and user acceptance testing processes.

Contractual Liability to your customers

Often there are contractual gaps between what your suppliers will indemnify you for if they are unable to fulfil their obligations, and the liabilities and warranties you accept with your customers, if you are unable to fulfil your obligations. Some service providers, such as cloud providers, note in their terms and conditions that they are not liable for unanticipated or unscheduled downtime of all or a proportion of their services for any reason. Keep this in mind when you consider it is common for many Software as a Service (SaaS) companies (who are supported by cloud providers both on their front and back end) to provide warranties and indemnities to their customers if they are unable to provide their services, without drawing reference in contract to service failures beyond their control.

How would you honour a guarantee to provide a service 98% of the time, where your operations remain totally reliant on third parties you have no influence or control over, where their failure is your failure?

How would you honour a guarantee to provide a service 98% of the time, where your operations remain totally reliant on third parties you have no influence or control over, where their failure is your failure?

Most parties often end up taking on more liability than is realistically necessary, and this can be due to many factors: for smaller companies with less bargaining power, pressure to acquire more valuable business deals may incentivise some to accept greater liability than normal. Often they will agree to accept their customers' terms and conditions, which are obviously written in favour of their customer rather than applying their own terms and conditions of trade. Hence, it's essential that when preparing service contracts you seek to include clauses that limit your liability to events realistically within your control and that these terms and conditions are standard within your own terms of trade.

As mentioned above, the contracts entered into by technology companies are often heavily in favour of their client. These contracts may request the supplier of the technology product/service to assume contracted liability to a greater level of responsibility and duty of care than is reasonably needed. The contract may also specify a greater level of compensation than is reasonable. There may be punitive conditions such as paying compensation to your client for not hitting a critical milestone on time, an exposure which is not typically covered under insurance.

Other examples of assumed liability that should be considered before accepting include:

- Accepting liability without proof of fault
- Extending liability to cover acts or omissions of third parties
- Agreeing to perform services to "the highest international standards and practices"
- Providing excessive indemnities or hold harmless obligations
- Agreeing to provide deliverables of "the best quality".

Other scenarios may arise where the technology supplier assumes liability above what the law would otherwise require. For example, agreeing that the supplier will be liable for any delays, even where the delay is beyond the supplier's reasonable control, such as cloud failure or system outage.

Also important to consider are pre-contractual representations or other conduct outside of a contract, where liability may also be assumed without real thought.

Jurisdiction Conditions

New Zealand technology businesses have had amazing success in offshore jurisdictions, such as North America, Asia and Europe. With entry into these markets there are additional considerations around local legislation and requirements. What may be acceptable to include in your standard terms and conditions in New Zealand may not be acceptable or legal to include in an offshore jurisdiction.

You may also have to agree to local jurisdiction in relation to any dispute or litigation that may arise due to the failure to supply your technology services as promised. This can be complicated further when dealing in North America, where your subsidiary company might be based in California, your client in New York State, and the jurisdiction for any disputes being in Texas. Often where a customer and client can't agree on local jurisdiction, an independent jurisdiction will be chosen. Furthermore, given the litigious nature of some of these offshore markets, what might typically be accepted in New Zealand – not hitting critical milestones, but the scope creep being accepted by both parties, may lead straight to a dispute resolution procedure in an offshore jurisdiction, with substantial costs being incurred. Our global experience has seen huge multi-million dollar claims against non-USA firms naively entering into the US market without weighing up the litigation costs versus the commercial benefits of expansion.

Cybersecurity Issues

If you're working in the IT industry, cybersecurity should form an intrinsic part of your operations and risk management. As a technology business, the biggest risk is an inability to provide your service, and cyber risks are often at the forefront of hindering your service delivery. In addition, a technology service provider has a legal obligation to provide a secure environment to protect any client data or information that is held by the company. Failure to cyber-proof your business and have adequate cyber risk mitigation plans can leave your business prone to extensive liability.

DDoS Attacks

While most technology businesses might not consider themselves likely to be prone to a distributed denial of service attack (DDoS), it is important to understand the wide-ranging implications of a DDoS attack on a technology company. A DDoS attack can simulate thousands and even millions of computers trying to access a website, flooding it with requests. The overload of access requests renders use of the website impossible, thus impairing it from providing its service.

A DDoS attack can simulate thousands and even millions of computers trying to access a website, flooding it with requests

Most technology companies operate with a value chain that can see various parts of the process outsourced or subcontracted to external parties. Where a DDoS attack creates cause for concern is in an event where one of the external parties is hit by a DDoS attack, which can disable certain functions of the business process, and sustain lost revenue and remediation costs.

With an estimated 35-45% of all DDoS attacks and mitigation incidents attributed to IT, SaaS and cloud service providers[30], few members of the New Zealand IT industry can afford to overlook their vulnerability to the ramifications of a DDoS attack. In addition to IaaS, SaaS and TaaS providers, other IT businesses are also vulnerable, such as e-commerce and online advertising companies, media companies and telecommunications providers[31]. With over 10 million DDoS attacks predicted in 2017[32] and a possible intensification of the Mirai attacks, DDoS attacks stand as arguably the leading cybersecurity issue for the year.

With over 10 million DDoS attacks predicted in 2017[32] and a possible intensification of the Mirai attacks, DDoS attacks stand as arguably the leading cybersecurity issue for the year

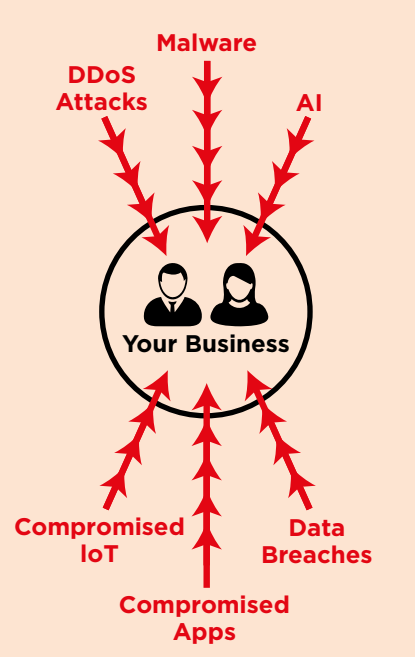
DDoS Attacks in the Cloud

When using private cloud computing, you are sharing the services with potentially millions of other customers you know nothing about. While you might not be considered a target for a DDoS attack, the same can't be said for all customers that you share the cloud environment with. Thus, cloud service users that are likely to be a target of a DDoS attack can inadvertently affect other unrelated users on the same network. When a DDoS attack is launched at a cloud service's data centre, there lies the risk of "spill-over", where other users' traffic is affected along with the primary target's usage of the cloud service[33]. For smaller cloud hosting services that might lack the infrastructure to fully repel a large, sustained DDoS attack, this causes significant problems both for the provider and the customers.

However, this does not discount the possibility of larger service providers suffering DDoS attacks. For example, a New Zealand website design and hosting company suffered a massive DDoS attack earlier this year aimed at one or more of their customers, which then caused website outages for several more customers, who the attack was not aimed at[34]. This sort of attack thus poses a significant danger for web hosting servers. Should they suffer such an attack, they are at a risk of compromising millions of dollars of lost revenue and business interruption on their clients' behalf, and would be forced to remediate immediately as well as provide some form of compensation to their clients. The customers' operations are also jeopardised as the targeting of specific customers can vicariously affect several other unrelated customers.

Internet of Things

The growing presence of Internet of Things (IoT) devices in the world is set to result in an escalation of the accumulation of data[35], at a rate where network security is always playing catch up to keep the Internet of Things secure. Vulnerable IoT devices with inadequate protection and pre-programmed passwords can be infiltrated and manipulated by malware to conduct DDoS attacks. There lies a significant risk in the cyber world of compromised IoT devices programmed into a botnet and being used to conduct attacks, as seen in the recent Mirai malware attacks[36]. The Mirai virus has been attributed to a spate of recent DDoS attacks across the world, from the blogs of cybersecurity specialists to internet service providers around the world. A recent report published by cybersecurity specialists Symantec noted the number of DDoS malware programs designed to infiltrate Linux-based firmware used in IoT devices is continuing to increase.



Potential cyber attacks on your business

A fundamental problem that lies with IoT security is that because most IoT devices generally have a primary function, interconnectivity is a supplementary feature. Thus, they cannot be relied to conform to the same level of security standards upheld by business IT networks and software. This creates a security issue when these interconnected, but vulnerable, devices remain connected to the Internet of Things. With smart device manufacturers consistently bringing new devices into the market, less attention will be paid in maintaining the network security of older device models[37]. Thus, older devices stand prone to having network vulnerabilities exploited. With an estimated 5.4 billion IoT connections predicted to be connected to the Internet by 2020, the scope of potential damage through cyber risks associated with the Internet of Things is profound.

Malware

Malware, short for malicious software, is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. With the rising number of IoT devices incorporated into business operations, remote access granted to employees and increased connectivity of systems and layers through application programming interfaces (API), the risk of your business being compromised through malware is increased further.

Artificial Intelligence (AI)

A relatively new cyber threat to technology businesses is AI-powered cyberattacks, which will make fighting hackers even harder. Machine learning algorithms are increasingly being used by cyber criminals to monitor and learn from emails, social media profiles, photos accounts, video streaming and online shopping accounts. The more information that is available to sift through, the easier it would be for an AI to learn about the victims' behaviours and habits, and exploit that in an effort to steal critical data such as propriety business information (e.g. IP and trade secrets), client lists and passwords. Just as big data and data mining are helping businesses to become more efficient and targeted with their services, it is also helping cyber criminals to do the same. As this new technology develops, we're likely to see an increase in incidents.

Just as big data and data mining are helping businesses to become more efficient and targeted with their services, it is also helping cyber criminals to do the same

Data Breaches

With increased incidents of ransomware and other forms of malware encrypting, deleting, corrupting, modifying and releasing data, data breaches will continue exposing technology companies to significant risk. A more recent phenomenon is hackers targeting businesses and data storage facilities and other businesses who hold large data sets and wiping the data. This differs from other attacks where often a ransom is requested to unencrypt the data or prevent its release. In these new incidents we are seeing the hacker typically instructs the administrators of the data to secure their deployments in the future, after deleting all historic data sets.

What's sometimes forgotten as a data or cyber risk is liability arising from simple human errors. Incorrectly entered data or improper use of critical information can result in substantial litigation.

What's sometimes forgotten as a data or cyber risk is liability arising from simple human errors. Incorrectly entered data or improper use of critical information can result in substantial litigation

Human error is believed to be the leading cause of data breaches, followed by malware and phishing and can arise when:

- Employees leave unencrypted or unsecure laptops in unlocked cars or public places
- Employees given access to systems and information beyond which is necessary for their role
- Access not removed when an employee resigns or terminated
- Sensitive data emailed to an unintended person
- Developers inadvertently configuring a databased containing sensitive data, which is internet-facing and searchable through Google[38]

Risk Management Strategies

With the ever increasing reliance on third party suppliers to support your business, evolving cyber threats and the interconnectivity of systems (both B2B and B2C), it is essential to understand these risks and safeguard your company. The following section provides commentary on strategies than can be implemented to help manage and understand the common risks that technology companies face.

Scope Creep

Any technology company that has been in business for any length of time has experienced the monster that is scope creep. Once scope creep has occurred it can be very difficult to recover from. Even if you haven't had to hand over or refund fees to your client, if punitive conditions exist in your contract for not hitting critical milestones the result is still the same:

More time and resources allocated to a project	=	**Additional cost and less bottom line profit**

In a worst-case scenario where scope creep leads to the non-delivery of a technology solution for a client, expensive litigation can arise as well as end a historically profitable business relationship. In the most devastating scenario, if the project failure is in the public domain, it can result in the insolvency of your business.

A small amount of scope creep is generally accepted and can be managed if done correctly. To limit the level of scope creep, risk management measures should be implemented:

Understand the outcome

You must have a solid, clearly defined understanding of what the client wants to achieve. If you understand the outcome then you should have a relatively clear idea of what you what is needed in order to fulfil the client's requirements before you have even discussed specific details.

Define the scope and set milestones

Clearly defining the scope of works so that both parties understand and agree on what will be delivered, in what time and at what cost is critical. Breaking down the project into milestones with achievable deadlines[39] can help you stick to schedule and prevent veering away from the original plans. These milestone plans can be as detailed as necessary, and will encourage the project manager to stay on track.

Put everything in writing

Once you understand the outcome and have clearly defined the scope of work and the proposed price, it is vitally important the client reads, understands and signs off all necessary documentation.

One common issue that often arises are arguments between a technology services provider and a customer as to what changes fall within scope of the original project and what changes constitute a "change request" (which falls outside of the original scope and often attracts additional charges to the customer). The customer will always try to argue the change falls within scope so they don't incur additional costs, whereas the supplier will argue it is additional work, as they have to allocate additional resources and incur additional costs which were not previously accounted for. This can be complicated further where multiple parties exist in a project, all with different terms and conditions within their contract.

Contractual Liability

It is common sense that any technology company should attempt to limit their obligations and liabilities as much as is commercially and legally possible, such as minimising acceptance criteria and having appropriate limitation of liability clauses. However, it can be tempting for a technology supplier to make generous (perhaps overly generous) representations and commitments to a customer in the hope of closing a deal. It may also be commercially necessary and appropriate in the right circumstances to agree to be held to a higher standard or greater potential liability than the law would normally impose for the right client (eg. where a very large prospective customer is able to wield significant bargaining power).

It can be tempting for a technology supplier to make overly generous representations and commitments to a customer in the hope of closing a deal

However before agreeing to any additional obligations technology suppliers should:

- Understand what additional specific risks and liabilities you will be committing to, and the potential insurance and other implications that may arise.
- Consider whether the heightened obligation is truly necessary and appropriate, or whether a lesser obligation can be negotiated
- Consider the potential scope of indemnity/ "hold harmless" clauses and third party liabilities, whether they are appropriate in the circumstances, and whether they can be limited or removed.
- Expressly define quality requirements. Instead of committing to potentially vague concepts such as "high quality", "highest industry standard", or even "best practices" the contract should define the specific standard or practices the technology company must achieve. This reduces uncertainty for both parties, and is good practice regardless of insurance and other implications.
- Make sure the contract contains a dispute resolution clause, that is fully understood by both parties
- Where possible exclude liquidated damages and other punitive conditions

Force majeure clauses

Force majeure clauses are often used to exclude liability from incidents known as "acts of God", where detrimental incidents are unforeseeable or unpreventable. Technology companies utilizing third party service providers such as cloud providers, ISP's, telecommunication companies and power companies should always look to exclude liability arising from such failures by incorporating force majeure clauses into their service contracts.

Other contract conditions

In addition to force majeure clauses it is also prudent to exclude liability where possible from events such as hardware failure, third party software failure, computer virus, DDoS attacks and even operating system failure, which can result in a delay or failure to provide your technology services, often through no fault of your own. It is also recommended to exclude liability for any breaches of intellectual property committed by third parties if possible, provided that you are unaware of any such breaches taking place.

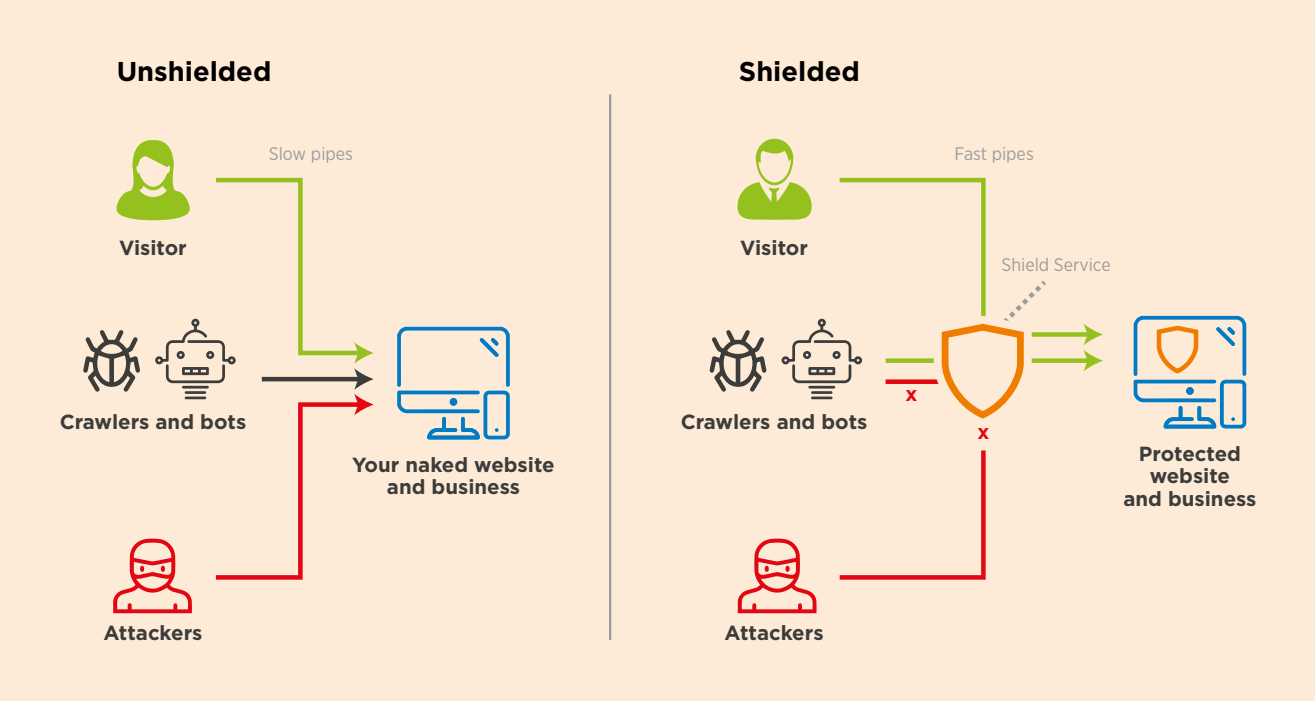
Special attention should be given to force majeure or other contract conditions specified in any contract you are asked to agree to.

Special attention should be given to force majeure or other contract conditions specified in any contract you are asked to agree to

Cyber Risk Management Strategies

DDoS Attacks

Shielding DDoS Attacks: In order to circumvent DDoS attacks, many companies have launched or started using anti-DDoS attack shields to protect their operations[40]. IT companies such as Cloudflare and Red Shield offer specific shield services to businesses to protect them from DDoS attacks. Utilising such services can form an integral part of your cybersecurity measures, particularly if your business provides services such as Technology-as-a-Service (TaaS) or Software-as-a-Service (SaaS), where a DDoS attack of your system could result in an inability to provide your technology services or products to your customers.



Disaster Scenario Simulations

The opportunity to run disaster scenarios and incident response simulations should be utilised to further cyber-proof your business and ensure your infrastructure is adequate to combat the repercussions of cyber security incidents.

While it's one thing to formulate disaster scenarios and incidence response plans, it's another thing entirely to execute these plans routinely. Given the constant evolution of technology, your contingency plans risk being outdated at the time of an incident. It's prudent to practice trial runs of your contingency plans at least once a year, and conduct a thorough evaluation of the plans' effectiveness.

Pen Testing

Short for penetration testing, pen testing aims to test the strength and hardness of the security of a computer system by attempting to infiltrate the system and expose any bugs or weaknesses. It can involve the use of hackers[41] who try to access your system with background and system information (white box) or with only very basic or no information (black box). What makes pen testing useful is that if done correctly, it will always yield some results. No system is fool-proof, and pen testing can thus be used to exploit any chinks in the armour.

In addition to testing the vulnerabilities of your system, pen testing provides employees with valuable experience in responding to an external attack on their systems and provides the opportunity to test your own internal controls in the outbreak of such an event. Hence, pen testing can be incorporated into your incident response plan and disaster simulation training, ensuring that your infrastructure and staff are robust enough to withstand large-scale cyber incidents.

The value pen tests can add to your business is profound:

- Tests can identify higher-risk vulnerabilities and help prioritize the vulnerabilities that need the greatest immediate attention[42]
- Tests the ability of network defenders to successfully detect and respond to the attacks
- Tests the effectiveness of your security controls

It is recommended that tech businesses of all sizes opt for pen testing if they have the available resources to do so. The majority of risk management consists of preventative techniques, and the pre-emptive nature of penetration testing fits this approach.

Bug Bounty Program

A bug bounty program incentivises hackers to try and exploit weaknesses or bugs, which they can then claim a bounty from by notifying the developers. Bug bounties have increasingly been adopted by internet giants such as Google and Facebook, in response to the growing number of white hat hackers. Smaller companies are also increasingly adopting this risk management tool.

Security Monitoring

Organisations are now increasingly creating security monitoring applications that aim to alert clients of a cyberattack as soon as it happens. A common issue with cyber incidents such as data leaks and infiltration is that they are often discovered much later, or never discovered at all. Security monitoring service providers thus allows you to respond much quicker in the aftermath of a cyberattack, which can thus significantly reduce remedial costs. This is especially valuable in the event of data breaches: as more time passes between the incident and notifications/remedial action, the extent of liability and remediation costs can increase greatly.

Data Breaches

Multi region data hosting is recommended with at least daily backups of all systems in place should there be a loss of service in one of the data centres. Although the possibility of your operations suffering in the event of an earthquake is remote at best, it's recommended to avoid having data storage centres in the same area, in case a freak occurrence or weather conditions damage multiple centres located in the same area.

Honey Pots

A honeypot is a computer system that is set up to act as a decoy to lure cyberattackers, and to detect, deflect or study attempts to gain unauthorized access to information systems. Generally, it consists of a computer, applications, and data that simulate the behavior of a real system that appears to be part of a network but is actually isolated and closely monitored. All communications with a honeypot are considered hostile, as there's no reason for legitimate users to access a honeypot. The honeypot may also be used to monitor employee's behaviors and what access they have to a network, which possibly they should not have. Viewing and logging this activity can provide an insight into the level and types of threat a network infrastructure faces while distracting attackers away from assets of real value.

Technology Liability Insurance

With new technologies come new liabilities and as such technology liability policies more than any other form of insurance need to constantly be reviewed, updated and changed to respond to new technological exposures.

Insurers can respond to this in a number of ways:

- **Exclude the new exposure – Y2K, e-commerce exclusions, transmission of virus exclusions, terrorism exclusions broadened to exclude cyber terrorism; or**
- **Underwrite the new exposure and provide coverage and a claims response**

Contractual requirements in many instances also make insurance a compulsory purchase even where robust risk management already exists. Increasingly these third party contractual requirements in relation to insurance are becoming more specific around what the insurance must respond to and include. The days of just providing a certificate of insurance to your customer noting you hold public liability insurance of $1,000,000 are numbered.

The days of just providing a certificate of insurance to your customer noting you hold public liability insurance of $1,000,000 are numbered

It is now common in both in New Zealand and overseas for customers to request written proof that your insurance includes cover for the following before employing your services:

- **Cover for breach of network security**
- **Cover for release of personal information or proprietary data – whether non malicious human error or through a cyber-attack.**
- **Affirmative cover for cyber liability**
- **Higher limits of indemnity being required. In 2016 technology liability insurers increasingly saw contractual requirements to hold limits of indemnity (for Professional Indemnity and Public Liability Insurances) in excess of $10 million with limits in excess of $30 million being required where services are provided to larger clients and government departments.**
- **Confirmation you will continue to hold insurance specific to the work you have performed for your client for seven years post the completion of your project. Bear in mind this might be at the level of insurance mentioned above (e.g. $10 million, $30 million etc).**

With more and more companies putting total reliance on technology and the likelihood that technology solutions will also be core business solutions, there is a lot at stake if software fails or doesn't perform as promised. This can also be further complicated if you are dealing with offshore jurisdictions and time zones, which as indicated earlier is a common theme for New Zealand technology businesses.

With the costs and complexity of technology claims continuing to increase along with the reliance you place on third parties, it is crucial that technology liability insurance plays an intricate part of your risk management strategy now more than ever.

The below table provides a good overview of the typical benefits of an up to date technology liability policy relative to other insurance policies:

Business Liability Risks	Common Liability Insurance Policies		
	TECHNOLOGY LIABILITY	CYBER LIABILITY	PUBLIC LIABILITY
Errors or omissions in software coding	●	●	●
Cyber security issues causing loss to client	●	●	●
Project failure / Delay due to negligence	●	●	●
Contractual disputes	● But only in line with common law	●	●
Loss of client data due to negligence	●	●	●
Loss of client data due to cyber attack that technology company should have prevented	●	●	●
Physical damage to client's property	●	●	●
Physical damage to client's property arising from the transmission of a virus / malware	●	●	●
Bodily injury caused to third party	●	●	●
Bodily Injury caused to a third party arising from the transmission of a virus / malware	●	●	●
Business interruption suffered by tech company due to own systems being breached	● Only if there was also a third party client impact	●	●
Unintentional Intellectual Property infringement	●	●	●
Dishonesty or fraud committed by staff	● If it causes a third party loss	●	●
Breaches of fair trading legislation	●	●	●
Breach of Network Security (including DDoS) resulting in financial loss to your clients	● If a result of negligence	●	●
Inability to provide hosting services / SaaS / IaaS / PaaS to your clients	● If a result of negligence	●	●

● Cover provided ● No coverage

How does Technology Liability Insurance Work

The following examples detail several scenarios where an IT firm may face liability, and outlines the insurance response in the wake of such an event:

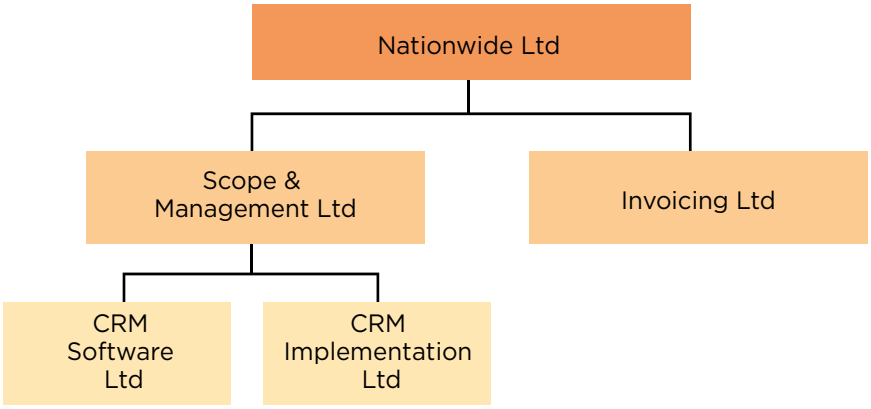
Scenario 1

This is an example of a typical large IT project structure, where failure of the project can give rise to a number of liability claims:

The project

- Nationwide Ltd is a large, multi-site nationwide organisation with many customers that requires a complex new CRM system to replace their existing, obsolete system.
- The new system must integrate with the client's existing invoicing and accounts system
- The existing invoicing and accounts system is supplied and maintained by Invoicing Ltd, and Nationwide has a longstanding, good relationship with them.
- Nationwide engages a firm of project consultants, Scope & Management Ltd, to scope and subsequently manage the project. The contract includes a number of interim milestones and a final delivery deadline of a year.
- Scope & Management sub-contracts with CRM Software Ltd to supply the new software.
- Scope & Management also sub-contracts with CRM Implementation Ltd, a company certified as a specialist in the CRM software, to implement the installation, including all of the configuration and customisation needed to fit the software to Nationwide's needs.
- Because of their existing relationship, Nationwide contracts directly with Invoicing Ltd for integration with the invoicing and accounting software.

> The contractual structure is therefore as follows:



The project encounters numerous problems:

1. The initial software supply contains bugs that are only discovered midway into the project. CRM Software Ltd, located overseas, is required to send representatives to New Zealand to fix the bugs and offer remediation advice to the client.
2. Difficulties arise in integrating the CRM and billing systems, and this is exacerbated by a lack of direct communication between the Invoicing Ltd and CRM Implementation Ltd. Each blame the other.
3. The employee in charge of the project at Scope & Management Ltd suffers a nervous breakdown and quits the project. A new manager with less experience in large projects is appointed.
4. It becomes apparent that the scoping was done inadequately with some incorrect assumptions made. There is scope creep, and a mid-way overhaul of the existing infrastructure. Nationwide is charged an additional $5 million ($2.5m by Scope & Management Ltd, $2.5m by CRM Implementation Ltd) for this additional work.
5. Delays are also caused by problems in testing. There is a lack of clarity over which party is responsible for different parts of the testing.
6. The project is delayed by a year, causing Nationwide Ltd to incur very significant additional staffing costs due to the need to continue to use the old, inefficient system, and also additional licencing costs.
7. Due to the delay of the project and extensive remediation required, Nationwide refuses to pay any costs beyond the original estimate. They also demand compensation of $10 million from Scope & Management Ltd.
8. Scope & Management Ltd seeks to pass the blame onto all the other parties.

The insurance position

- Scope & Management Ltd holds liability insurance of $100 million.
- CRM Software Ltd holds liability insurance $10 million.
- CRM Implementation Ltd has liability insurance of $500,000.
- Invoicing Ltd has liability insurance of $1 million.

The result

Because there are multiple causes of the delays, it is extremely difficult to attribute any particular delay to a failing by one particular party. Each party incurs many hundreds of thousands of dollars investigating the causes. The complexity of the situation means it is almost impossible for any of them to prove that they were not at least partly responsible for the situation. After much arguing about the best way of resolving the dispute, all of the parties attend a mediation. Although each party disputes exactly who is at fault, it is generally agreed that Scope & Management are more to blame than others and that CRM Software have only contributed a little to the problem. CRM Implementation are in financial difficulties as a result of the non-payment of their invoices, and cannot afford to pay anything over their insurance limit.

The complexity of the situation means it is almost impossible for any of them to prove that they were not at least partly responsible for the situation

- **Nationwide** accepts a compensation payment of $5 million and an agreement that the invoices for the additional work will be written off.
- **Scope & Management Ltd** writes off their $2.5m of additional work. This is not covered by insurance. They also contribute $3m to the compensation payment, and this is paid by their insurer.
- **CRM Implementation Ltd** contributes $500,000, which is paid by their insurer. They write off their $2.5m of additional work. This results in their becoming insolvent and going into liquidation soon afterwards.
- **CRM Software Ltd** contributes $1m towards the claim for compensation, which is paid by their insurer. This is more than they ought to be liable for, but because CRM Implementation Ltd is in financial difficulties they are forced to pay the shortfall to get the claim settled and to protect the reputation of their software.
- **Invoicing Ltd** contribute $1m to the settlement, which is paid by their insurer.

Scenario 2

A service provider based in Australia offers software solutions and cloud hosting services for financial advisers in New Zealand. They suffer a power outage due to thunderstorms that fry their hardware and leave their systems offline for 3 weeks. This results in hundreds of financial advisers in

New Zealand left unable to use their systems. The advisers are unable to carry out investments for their clients, such as selling shares, and face claims by their clients for losses suffered. The advisers pass the cost of these claims on to the cloud service provider as a claim for breach of contract.

The insurance response

The extent to which the service provider is liable will depend on the terms of the contract. They might have a 'force majeure' clause and this will prevent them from being liable. They might also have a limitation of liability clause which limits their liability to a refund of fees, or to direct losses only. If they are liable, then their technology liability policy would meet the claims.

Scenario 3

A software development company uses a plugin from a major software supplier for one element of their product. When supplying the product to their customers, they warrant that all appropriate licences have been obtained. By mistake, it turns out they used the full version of the plugin rather than the basic version which was all that they had a licence for, and was all that was needed. The major software supplier pursues several of the end customers for licence fees and penalties.
The customers seek to pass this cost on to the software company.

The insurance response

The policy will respond to the claims by the customers for the additional licencing costs incurred. The software company will have to correct the software at their own cost so that it just uses the basic version in the future.

Scenario 4

An IT service provider provides and maintains the network infrastructure for a law firm. They attend the firm one evening to carry out some maintenance on the server. Due to errors made in the maintenance work, the firm discovers the following morning that the network is not functioning. It takes over a day to get it running again, but in the meantime the law firm has been unable to access its account system and as a result has failed to transfer funds for a number of property settlements, resulting in some of the property sales falling through and penalty interest being incurred on others. They have some very aggrieved clients. The law firm seeks to pass on these costs to the IT service provider and also terminates the support contract with them.

The insurance response

The IT service provider's liability insurance will respond to the claim by the law firm.

Conclusion

The ever-expanding scope of technology stands as both the industry's greatest strength and weakness. As New Zealand technology businesses continue to expand their operations in a more globalised world, their exposure to liability risks increase in turn. Operating in a more globally interconnected business world not only increases risks to the trappings of overseas jurisdictions, but can leave businesses vulnerable to a greater amount of cyber-risks. The constantly evolving nature of the technology industry results in constantly evolving cyber threats, with each wave of cyber risks becoming more sophisticated and potent than its predecessor.

No industry is liability-proof, and the technology sector certainly is no exception. Despite your best risk mitigation efforts, an incident incurring technology liability can arise. It is here that tailored, up to date technology insurance policies aim to fill in the gaps of normal and out of date coverage, and protect businesses from incurring substantial financial and reputational losses. With the industry steadily adapting to the new challenges imposed by technological risk, there stands a greater likelihood of technology firms receiving more bespoke technology liability policies tailored to fit the needs of their business. Thus, technology liability insurance can provide the insured with a broad range of cover that includes coverage for professional indemnity, public liability and cyber issues.

Here at Delta Insurance, we believe that sound risk management strategies which address new and evolving forms of risk are at the forefront of protecting your business. Dovetailing into these risk management strategies should be insurance coverage that is also constantly evolving to address these new and varied exposures that technology companies face, as even with the most robust risk management procedures, litigation and disputes can still arise. Collectively, through proactive thinking, planning and innovation, we can manage these risks and threats together and continue to make sure that New Zealand technology companies remain at the forefront of the world stage.

Sources

1. Ryan, Holly. "Tech sector cracks $1 billion in growth". The New Zealand Herald. Oct. 19, 2016. http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11732068
2. "Information and Communications Technology". NZTE. https://www.nzte.govt.nz/en/buy/our-sectors/information-and-communications-technology
3. MBIE Sectors . ICT Report 2015. New Zealand: Ministry of Business, Information and Employment, 2015. http://www.mbie.govt.nz/info-services/business/business-growth-agenda/sectors-reports-series/information-and-communications-technology-report
4. MBIE. High Technology Manufacturing Report 2013. New Zealand: Ministry of Business, Information and Employment, 2013. http://www.nztech.org.nz/wp-content/uploads/2014/10/MBIE-HiTech-sector.pdf
5. "High Tech in New Zealand." Workhere New Zealand. Accessed Jan. 27, 2017. http://www.workhere.co.nz/industry/high-tech/about
6. NZTech. From Tech Sector to Digital Nation. New Zealand: New Zealand Technology Industry Association, 2016.
7. Shanahan, Greg. "State of the sector: technology." Idealog. Aug. 12, 2016. http://idealog.co.nz/tech/2016/08/state-sector-technology
8. TIN 100 Technology Industry Analysis New Zealand (2016 report). New Zealand: Technology Investment Network, 2016.
9. "World-first Kiwi robotics technology set to take on Europe." Scoop.co.nz. 24 May, 2016. http://www.scoop.co.nz/stories/BU1605/S00728/world-first-kiwi-robotics-technology-set-to-take-on-europe.htm
10. Henderson, James. "Expanding Kiwi software firm jumps feet first in Vietnam venture." Reseller. 19 July, 2016. http://www.reseller.co.nz/article/603630/expanding-kiwi-software-firm-jumps-feet-first-vietnam-venture/
11. "5 project management blunders to avoid." CeBIT Australia. Accessed 30 Jan., 2016. http://blog.cebit.com.au/5-it-project-management-blunders-to-avoid
12. Fletcher, Hamish. "Spark owed $26m by troubled Mako Networks". The New Zealand Herald. Aug. 24, 2015. http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11502019
13. "What is Gold Plating in Project Management?" Project Management Learning. March 5, 2010. http://www.projectmanagementlearning.com/what-is-gold-plating-in-project-management.html
14. Ludlow, Mark. "IBM 'negligent and misleading', Queensland alleges". The Australian Financial Review. Aug. 23, 2015. http://www.afr.com/technology/enterprise-it/ibm-negligent-and-misleading-queensland-alleges-20150820-gj42md
15. Cowan, Paris. "Queensland's IBM ban lives on". Itnews.com.au. June 20, 2016. https://www.itnews.com.au/news/queenslands-ibm-ban-lives-on-420969
16. Leung, Peter. "IP Litigation is a big deal in Asia". Managing Intellectual Property. Dec. 03, 2013. http://www.managingip.com/Blog/3285152/IP-litigation-is-a-big-deal-in-Asia.html
17. Eppenauer, Bart. "Emerging Antitrust Regulation of Intellectual Property Licensing in Asia". Ipwatchdog.com. Aug. 16, 2015. http://www.ipwatchdog.com/2015/08/16/emerging-antitrust-regulation-of-intellectual-property-licensing-in-asia/id=60693/
18. Thomson, Chris. "A newfound patent passion". Asian Legal Business. Sep. 30, 2016. http://www.legalbusinessonline.com/features/newfound-patent-passion/73175
19. Keall, Chris. "Phitek settles with Bose". National Business Review. Nov. 19, 2008. https://www.nbr.co.nz/article/phitek-settles-with-bose-38022
20. Open Invention Network. Accessed 16 Jan, 2017. http://www.openinventionnetwork.com/
21. Putt, Sarah. "Zeacom founder on the US, patent trolls and why he didn't float the company". Computerworld New Zealand. Jan. 30, 2013. http://www.computerworld.co.nz/article/452263/zeacom_founder_us_patent_trolls_why_he_didn_t_float_company/
22. Heinzl, Mark & Sharma, Amol. "RIM to Pay NTP $612.5 Million To Settle Blackberry Patent Suit". The Wall Street Journal. Mar. 4, 2006. https://www.wsj.com/articles/SB114142276287788965
23. Nakashima, Ryan. "NYTimes leads group defense in mobile patent suit". Associated Press. Aug. 28, 2012. http://usatoday30.usatoday.com/money/media/story/2012-08-28/mobile-patent-suit-New-York-Times/57368374/1
24. Bartz, Diane. "Patent licenser Helferich wins court round against New York Times, others". Reuters. Feb. 10, 2015. www.reuters.com/article/helferich-new-york-times-patent-idUSL1N0VK2BU20150210
25. Hatch, Patrick & Biggs, Tim. "Banks, websites down as wild weather knocks out Amazon Web Services". The Australian Financial Review. June 6, 2016. http://www.afr.com/technology/banks-websites-down-as-wild-weather-knocks-out-amazon-web-services-20160605-gpc8ob
26. Gray, Maryvonne. "UK power outage leaves NZ brokers unable to work". Insurance Business Online. Aug. 31, 2016. http://www.insurancebusinessonline.co.nz/nz/news/breaking-news/uk-power-outage-leaves-nz-brokers-unable-to-work-222475.aspx
27. "SSP outage: brokers consider compo claim". Insurance Business Online. Sep. 26, 2016. http://www.insurancebusinessonline.co.nz/nz/news/breaking-news/ssp-outage-brokers-consider-compo-claim-223937.aspx
28. Sumroy, Rob & Ives, David. "BSkyB v EDS". Slaughter and May. Feb 2010. www.slaughterandmay.com/media/926429/bskyb%20v%20eds_feb_2010.pdf

29. Sonne, Paul. "BSkyB Settles Claim Against EDS". The Wall Street Journal. June 15, 2010. https://www.wsj.com/articles/SB10001424052748703303904575292740970784182
30. "Q3 2016 DDoS Attack Trends". Verisign.com. 2016. https://www.verisign.com/assets/infographic-ddos-trends-Q32016.pdf
31. Verisign. Verisign Distributed Denial of Service Trends Report. (Volume 3, Issue 2 – 2nd Quarter 2016). USA: Verisign, 2016. https://www.verisign.com/assets/report-ddos-trends-Q22016.pdf
32. Deloitte. Technology, Media and Telecommunications Predictions 2017. London: Deloitte, 2017. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-deloitte-2017-tmt-predictions.pdf
33. Bradbury, Danny. "DDoS, the cloud and you". The Register. Jul. 21, 2016. http://www.theregister.co.uk/2016/07/21/ddos_the_cloud_and_you/
34. Sharpe, Marty. "Customers of large NZ website company Zeald have been hit by cyber attack". Stuff.co.nz. Mar. 4, 2016. http://www.stuff.co.nz/technology/77539929/Customers-of-large-NZ-website-company-Zeald-have-been-hit-by-cyber-attack
35. The White House. Cybersecurity Report. Accessed Nov. 15, 2016. https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf
36. Russon, Mary-Ann. "Largest ever DDoS attack: Hacker makes Mirai IoT botnet source code public". International Business Times. Oct. 13, 2016. http://www.ibtimes.co.uk/largest-ever-ddos-attack-hacker-makes-mirai-iot-botnet-source-code-public-1584579
37. Hajdarbegovic, Nermin. "Are We Creating An Insecure Internet of Things(IoT)? Security Challenges and Concerns". Toptotal. Accessed Feb. 1, 2017. https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things
38. http://www.cybersecuritytrend.com/topics/cyber-security/articles/421821-human-error-to-blame-most-breaches.htm
39. "Managing Scope Creep in Project Management". Villanova University. Accessed Feb. 3, 2017. www.villanovau.com/resources/project-management/project-management-scope-creep/#.WD8xTuZ942x
40. Lardinois, Frederic. "AWS launches Shield to protect web applications from DDoS attacks". Techcrunch. Dec. 1, 2016. https://techcrunch.com/2016/12/01/aws-launches-shield-to-protect-web-applications-from-ddos-attacks/
41. Pearson, Alan. "What is Penetration Testing and Why is It Important". Security Innovation Europe. Mar. 20, 2014. http://www.securityinnovationeurope.com/blog/what-is-penetration-testing-and-why-is-it-important
42. Basu, Eric. "What Is A Penetration Test And Why Would I Need One For My Company?". Forbes. Oct. 13, 2013. http://www.forbes.com/sites/ericbasu/2013/10/13/what-is-a-penetration-test-and-why-would-i-need-one-for-my-company/#53406bc342da

Delta Insurance New Zealand Limited

Recent events both in New Zealand and around the globe demonstrate the rapid and sometimes surprising pace at which change takes place. Businesses today need to be on their toes and actively responding to a host of new and developing risks. They need an insurance partner who can provide certainty in an ever changing world. Unfortunately, some events have consequences that can't be anticipated – accidents, mistakes, bad decisions or external events outside the control of a business. Businesses owe it to their stakeholders, their clients and the general public to manage risk effectively. It's important that as a business owner, you are confident that you and your business are reasonably protected against possible eventualities. Delta Insurance is proud to be the only locally owned and operated specialist liability underwriting agency in New Zealand. We provide comprehensive insurance coverage solutions with a range of liability products in both the financial lines and casualty insurance sectors. Delta Insurance accesses capacity via Lloyd's of London. Delta Insurance is a Lloyd's Coverholder. As a local Kiwi company, we want to be a change leader in the local industry. Delta... symbol for change.

Our brokers and clients

As the leading provider of technology liability insurance in New Zealand, Delta Insurance would like to acknowledge and thank our brokers and our clients who have welcomed us into their offices and given generously of their time to share with us what they deal with at the coalface everyday. Many of the issues and strategies outlined in this white paper have originated from these meetings. By working closely with our Insureds, we gain a better understanding of their world and their challenges so that we can provide them with the appropriate liability cover they need to conduct their business effectively.

Delta Insurance

Level 8, 57 Fort Street, Auckland 1010

PO Box 106 276, Auckland 1143

P +64 9 300 3079

deltainsurance.co.nz