Cyber-attacks:
Will your business be NZXT?

DDoS hit on NZ Stock Exchange emphasises need for robust cyber-risk governance

In the last full trading week of August 2020, several key markets of the New Zealand Stock Exchange were taken offline by "volumetric distributed denial of service" (DDoS) attacks from outside New Zealand that interrupted trading on four consecutive days. The NZX was required to halt trading on its Main Board, Debt Market and Fonterra Shareholders Market and the NZX website was down for significant periods during the tail end of reporting season and had to work closely with its network service provider Spark and the GCSB to resolve network connectivity issues.

Not only has this led to serious concerns regarding NZX's resilience, its vulnerability to cyber-risks and its reliance on Spark, it is also bringing into sharp focus the need for enterprises of all shapes and sizes to examine their internal processes around cyber-risk.

Wait, what is a DDoS attack?

A DDoS attack floods a machine or network with requests for information from multiple sources in a bid to overload it and stop other legitimate users from having their system calls fulfilled. DDoS attacks are hard to track down, because they're commonly embedded in malware such as MyDoom, WannaCry and other viruses/worms which infect millions of host computers worldwide without the host owner's knowledge or consent, turning the computers into "zombies" on a botnet which execute commands at the attacker's bidding.

The wide variety, availability, low cost and effectiveness of DDoS attack tools means that modern businesses are at an ever-increasing risk of targeted compromises of their key systems. These frequently take the form of ransomware attacks, where cyber-attackers conduct low-level attacks against a system and warn the system owner that a more significant attack will be carried out if a ransom is not paid (in cryptocurrency, naturally).

They're coming for you

We do not know at this stage if the NZX cyber-attack is a ransomware scheme, but in the past many of the most prominent attacks have focused on the critical IT infrastructure of financial institutions, presumably in part because they have the deepest pockets. Indeed, the NZ government's cybersecurity team CertNZ issued an alert in November 2019 warning that they had reports of extortion attempts by a Russian group called "Fancy Bear" targeting companies within the NZ financial sector and demanding a ransom to avoid DDoS attacks. What's more, the Reserve Bank estimated in early 2020[1] that the anticipated costs of cyber-attacks for the banking and insurance sectors in New Zealand could be as much as NZ$134m annually.

As tempting as it may be to think cyber-attackers are not interested your business, that perception has well and truly shifted in 2020. Recent surveys in the US[2] and in NZ[3] suggest that the vast majority of SMEs have moved to some form of remote working as a result of COVID-19 and that most employees wish to continue working remotely at least part of the time after lockdowns. Employees who work from home are increasingly dependent on IT that might have less security than their work setup, with the result that now even small businesses are in the firing line. And cyber-criminals aren't just interested in the troves of customer data (such as credit card numbers) you may hold, but anything that could potentially be of commercial value, including customer lists, commercial contracts, business

[1] *Cyber incident cost estimates and the importance of building resilience*, Vol 84, No. 2 February 2020

[2] *Wall Street Journal / Vistage Small Business CEO survey*, May 2020

[3] *COVID-19 Remote Working Employee Pulse Survey*, University of Otago's Work Futures Otago Group, May 2020

Cyber-attacks: Will your business be NZXT?
(Continued)

plans (including acquisition strategies), source code, trade secrets and other intellectual property.

IBM estimates[4] that the average total cost of a data breach in 2020 is US$3.9 million and that this cost could be minimised if organisations thoroughly planned and prepared for cyber-attacks. So whether you are large or small, a giant financial services enterprise, an SME doing business through Facebook marketplace, or a government department, cyber-attacks are becoming more common and more diffuse. It is not a question of if, but when, so the time to prepare for it is now.

Managing risk before a cyber-attack

Happily, there are many steps that enterprises of all sizes can take to reduce the risk of a cyber-attack and its financial and reputational impact on your business. Here are some key do's and don'ts for you to consider before your enterprise is cyber-attacked:

- **DO** discuss cybersecurity around the board table – as the Institute of Directors succinctly said it, "*put cybersecurity on the agenda before it becomes the agenda*"[5]. Cyber-risk is not just an IT issue but presents risks enterprise-wide, particularly given our increasing dependence on both IT and always-on connectivity. Directors should:
    - put in place a **cyber-risk framework** that allocates responsibility for risk-related governance functions (preferably to a cross-departmental cyber-risk team), identifies the roles and responsibilities within the organisation for when a cyber-attack occurs, and provides for regular reporting to the board;
    - adopt a documented **incident response plan (IRP)** which clearly defines the pre-planned series of actions that are put in motion when a cyber-attack occurs (usually in the form of "runbooks") as well as notification lines and escalation rules;
    - test the framework and IRP regularly to ensure they are understood and fit for purpose;
    - understand the legal, regulatory and contractual environment in which their business is operating; and
    - bring in expertise from external advisors (such as cybersecurity firms, forensic accountants or lawyers) to board discussions around cyber-risk wherever necessary.
- **DO NOT** shy away on the basis of cost. It may seem, particularly for smaller businesses, that the financial cost of guarding against a cyber-attack is too high for what is perceived as minimal risk (even though the level of risk will clearly vary from business to business). The market is shifting all the time, and SMEs can now consider using a lower-cost DDoS protection-as-a-service platform, while larger businesses might consider deploying an on-premises solution for their network;
- **DO** regular exercises in risk assessment and categorisation. This might start with an internal audit of not only the existing IT security processes you have in place but of the various categories of data your entity collects and holds. Ask yourself what is your critical IT infrastructure? What are your key intangible assets such as data or trade secrets and where are they stored? Who can access them? Regularly review the contractual protections you have in place with your third party IT service providers in relation to management of cyber-risk. An audit may expose gaps in the security structure and enable you to allocate your resources to where they will have the greatest impact. You cannot shield your business completely from risk, but you can do a cost-benefit analysis to identify which risks to avoid, which to accept and which to mitigate or

[4] *Cost of a Data Breach Report*[2020] (https://www.ibm.com/security/data-breach)
[5] *Cyber-Risk Practice Guide*, 2015

transfer to third parties (such as through suitable contractual provisions with your service providers or through insurance).

- **DO NOT** assume your cyber-risk insurance policy will answer. There are very often exclusions and conditions that apply, as well as other requirements to comply with (e.g. you have to use pre-approved service providers for incident response) before you can invoke the policy. Talk to your insurance broker to ensure the policy is fit for purpose and covers the critical risks identified as part of your risk assessment and categorisation exercise. Take legal advice where necessary.

Crisis management after a cyber-attack

If your business has been the subject of a cyber-attack:

- **DO** work through your IRP quickly and methodically, as time will be critical in determining what the ultimate impact will be on your business. The longer it goes on for, the greater the financial and reputational impact on your business and operations.
- **DO NOT** keep it quiet – you will naturally wish to control the public messaging around higher profile attacks, which is fine. But you will most likely have an obligation to notify your insurers within a strict timeframe (check your cyber-risk policy), and if you fail to do so your claim is likely to be declined. If the cyber-attack involves the compromise of personal information (such as customer and/or credit card information) and causes serious harm or is likely to do so, then you will also have mandatory breach reporting obligations (both to the Privacy Commissioner as well as the persons affected) under the Privacy Act 2020 when it comes into force on 1 December 2020.
- **DO** conduct a post-mortem on how your business performed during the incident. Try to identify any additions or amendments to your IRP and other internal processes that would enhance the effectiveness of those procedures. Learn from each incident and try to continually improve so that you are better prepared to defuse the next attack.
- **DO NOT** pay the ransom – you will be forever marked as an easy target for future ransomware attacks.

Want to know more?

If you have any questions about preparing your business for cyber-attacks, including best practice procurement of IT systems and services, or management of data security incidents, please contact our specialist Technology & Digital Team.