There has been an influx of cyberattacks and breaches recently throughout New Zealand. Cybersecurity Ventures estimate a new ransomware attack will hit every 11 seconds in 2021. Since moving to Alert Level 4, we've seen attacks on a number of NZ organizations hit with outages causing frustration among many. While they have contained the threats and continue to recover, the Government's Computer Emergency Response Team (CERT NZ) states,

*"DDoS attacks are not new, and most are repelled by organisations working with their service providers who are best placed to implement technical mitigations."*

With the reliance on digital services and devices, many businesses are working from home, It's important to shed light on the matter as the international threatscape is changing globally. If this is to be the norm for businesses and organisations, are we prepared?

## What and why you should care

It's important to understand and differentiate the kind of attacks that can happen. DDoS (Distributed Denial of Service) attacks are a full-frontal assault on an organization's servers. The hacker will overwhelm a site by summoning thousands or millions of bots to connect all at once, causing congestion and rendering it inaccessible. Different from a traditional hack, DDoS attacks have no element of breaking into servers or stealing data, while this method of data attack has been around for decades, they have grown due to being easy to pull off compared to a traditional hack of computer networks. Traditional hacks are a lot more sophisticated and will target important data. These malicious attacks could enable the loss of personal information, confidential records, company assets, income, productivity, and good will. Many organisations do not like to shed light on such incidents as it can subjugate and can jeopardies their image, letting down customers and shareholders in the process.

Both forms of ransomware attacks have no interest as to whom they target, as we have seen in the attack on the Waikato DHB earlier this year, there is no limit as to where or whom they will target next. Your best course of action is awareness, and how to prepare for them. Consider how much your servers can handle in case of such an attack or breach and review your security protocols. Many organisations have opted to move to cloud-based servers, with experts citing that the country's current security infrastructure is 'far behind'. The NZX incident last year happened because the exchange was only just in the process of moving to cloud-based servers, the 'opportunistic' attack lasted for days.

## How it effects Payroll

Integrity1 puts its utmost prioritisation on security and privacy measures, with our own and our client's data. Payroll can be one of the many factors that get disrupted from an attack, and we have seen cases where payroll systems have been unavailable for payroll processing, meaning that payroll needs to be calculated externally to the payroll system. This impacts data integrity and the ability to maintain important accruals and cumulative

calculations that immediately force payroll into non-compliance with legislation and other agreed requirements, such as Taxation, Leave Payments, Leave Accruals, Child Support, Garnishee Deductions, Leave Accruals and Balances, Apprenticeship Hours, Secondments, Temporary Allowances & Deductions, etc. Given that such a large portion of the population relies on their regular pay, the effects of not being paid correctly are incredibly detrimental, as well as the cleanup of data once access to the system is restored. Overpayments can cause as much hardship as underpayments when payments are reconciled and employers attempt to recover overpayments. Personal information of employees is also an incredibly delicate matter, and information must be secure to prevent fraud via stolen data and identity theft. Such penalties for personal data and privacy breaches can be costly.

All Integtiy1 staff are required to sit and pass the Privacy Act 2020 course (at a minimum) and we have engaged an external company to provide training on cyber awareness to ensure staff are vigilant and know when to click or not click on emails/material and escalate any strange looking emails/material to our IT department and peers as quickly as possible.  We restrict any access to Client data and/or systems to trained employees only.

When it comes to our remediation payment projects, where we manage the co-ordination externally, of sensitive data/information for our clients' past employees (including banking details and several forms of ID), we use a custom-built, secure emailing solution designed specifically for volume emailing. Emails are encrypted at rest and in transit. Brute force DDoS attacks are also monitored and blocked. We have invested significant time and cost in developing a secure purpose-built website portal so that former employees can check entitlement and then apply for a remediation back payment. Significant investment has been made in ensuring the website and its data is secure to maximise security and privacy due to the type of information that is required to be collated. All Data is only held in New Zealand or Australia, encrypted at rest and backup, web traffic is also encrypted, via smart hidden links, log monitoring, and password encryption.

## What to do?

So what should you do If your organisation has been compromised by a cyberattack? Report it to CERTNZ, the government's computer emergency response team. Being a part of MBIE, CERTNZ provides extensive information regarding cyberattacks and has an alert page dedicated to highlighting current threats.

Report a cyber attack here.

If you have concerns around the security of your payroll data, whether stored in-house or in the cloud contact us for a payroll data and process security review.