Cyber incident

As you may know, Bell & Graham was the subject of a cybersecurity incident in January 2025.

Since being informed of the compromise, we have been working hard to understand the scope of what has happened and identify those impacted. We appreciate your patience as we work through this situation which has been a stressful one for our team.

This notice sets out what happened, how we have responded, and provides recommendations for steps you may wish to take in response.

What happened?

In January 2025, upon our return to the office from the holiday break, Bell & Graham detected its server had suffered a cyberattack. Once this was discovered we took immediate steps to secure our systems and investigate the situation. This included engaging an external forensic specialist to investigate the scope of any compromise. We also notified the Office of the Privacy Commissioner and the New Zealand Police.

Our investigations have now revealed that some files held on our on-premises server were taken by the third party. We also understand that these files have been posted to a data leak site on the dark web.

Impact on client information

Our review of incident has identified that various client information was present in the exfiltrated dataset.

We note that the compromise did not impact our live client management systems, which is held on a cloud platform. Rather it impacted our on-premises server. Unfortunately, some client information is still held on this server. This includes information provided to us for our engagement or documents created for the purposes of completing work for our clients.

Where possible Bell & Graham has notified clients with live transactions to ensure these were not disrupted as a result of the incident. Unfortunately, in the interests of alerting people as soon as practicable it has not proved possible to reach out to all clients whose information may be impacted. If you are concerned about your information please contact us on lawyers@bellandgraham.co.nz and we can confirm whether your information is impacted.

What should I do?

Please do let us know if you would like confirmation as to whether your information is impacted. In the meantime, we would recommend all clients consider the below points as matters of general good practice:

- Stay alert to the prospects of fraud. We are mindful that scammers do take advantage of organisations through impersonation in order to elicit further details and access the affected community. Further information about common scams and frauds and what to look out for can be found on the 'Own your Online' website here.

- CERT NZ also provide a range of further material about securing your data more generally. Material for individuals can be found here.

- Regularly check your credit report for any suspicious entries. Information on how to check your credit report for free can be found here. Information relating to temporary suppression of your credit file can also be found here.

- Be wary of any correspondence, texts or phone calls purporting to be from entities you may engage with (such as law enforcement or your bank), that is asking to change bank accounts details or requesting funds. Always call the sender using an independently sourced number to confirm the legitimacy of any request.

- If you receive a text message or email that you think is spam, you can report this to Te Tari Taiwhenua (the Department of Internal Affairs) here.

- If you believe you are the victim of an online crime, then please report the matter to the Police dialling 105 (non-emergency reporting) in the first instance.

What if I have questions?

We understand you may have questions or concerns. Please do contact us on lawyers@bellandgraham.co.nz with any queries, comments or concerns you may have. You can also raise a complaint with the Office of the Privacy Commissioner.