KPMG

Reserve Bank of New Zealand Incident Assessment

Public Summary

May 2021

Contents

Disclaimers

Inherent Limitations

This Public Summary has been prepared in accordance with our Consultancy Service Order (CSO) between ourselves and the Reserve Bank of New Zealand (The Bank) and for no other purpose. The services provided under our Contract ('Services') have not been undertaken in accordance with any auditing, review or assurance standards. The term "Audit/Review" used in this report does not relate to an Audit/Review as defined under professional assurance standards.

The information presented in this Public Summary is based on that made available to us during our work for the Bank. Unless otherwise stated in this Public Summary, we have relied upon the truth, accuracy and completeness of any information provided or made available to us in connection with the Services without independently verifying it.

The statements and opinions expressed in this report have been made in good faith and on the basis that all relevant information for the purpose of preparing this Public Summary has been provided by the Bank and that all such information is true and accurate in all material aspects and not misleading by reason of omission or otherwise. Accordingly, neither KPMG nor their partners, directors, employees or agents, accept any responsibility or liability for any such information being inaccurate, incomplete, unreliable or not soundly based, or for any errors in the analysis, statements and opinions provided in this report resulting directly or indirectly from any such circumstances or from any assumptions upon which this Public Summary is based proving unjustified.

No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by the Bank as part of the process.

The Public Summary was prepared based on the information made available at the time. KPMG is under no obligation in any circumstance to update this Public Summary, in either oral or written form, for events occurring after the Public Summary has been issued in final form.

Third Party Reliance

This Public Summary is solely for the purpose set out in the Description of Services in the CSO and is not to be used for any other purpose or copied, distributed or quoted whether in whole or in part to any other party without KPMG's prior written consent.

Other than our responsibility to the Bank, neither KPMG nor any member or employee of KPMG assumes any responsibility, or liability of any kind, to any third party in connection with the provision of this Public Summary. Accordingly, any third party choosing to rely on this Public Summary does so at their own risk. KPMG expressly disclaim any and all liability for any loss or damage of whatever kind to any person acting on information contained in this report.

Internal Controls

The information provided has been evaluated through analysis, enquiry and review for the purpose of this Public Summary. KPMG does not warrant that these enquiries have identified or verified all of the matters which an audit, extensive examination or due diligence investigation might disclose. Due to the inherent limitations of any internal control structure it is possible that errors or irregularities may occur and not be detected. Our procedures were not designed to detect all weaknesses in control procedures and consequently we do not express an opinion on the effectiveness of the internal control structure.

Introduction and scope

Introduction

The Reserve Bank of New Zealand ("the Bank") requested that KPMG perform an assessment ("the Assessment") of the data breach that occurred in December 2020. This was to provide insights and recommendations to the Board, Governors and management on potential risk exposures, root causes and contributing factors in regard to information and critical systems management and associated security practices at the Bank related to the illegal breach of a third-party developed file transfer system, Accellion File Transfer Application (FTA) used by the Bank.

This Public Summary summarises our approach and the results of the work performed in accordance with the CSO agreed between the parties. Due to the nature of the incident, certain supporting information has not been included in this Public summary.

Objectives and Scope

The key objectives of the Assessment were to provide the Bank with:

1. An understanding and confirmation of the timeline of events and actions taken leading up to and in immediate response to the breach.
2. An assessment of the appropriateness of the incident response and actions taken to mitigate/remediate the breach, noting any perceived gaps or improvements.
3. Indications of any potential design or operating effectiveness control weaknesses that may have contributed to the breach, including any thematic or systemic issues in relation to:
    a. The level of awareness and action plans in place to address relevant outstanding audit findings, recommendations and Post Incident Process Improvements (PPIs).
    b. The robustness of current information management and information security technical, people and process related controls and their alignment with the Bank's risk appetite and enterprise risk register.
    c. Any relevant perceived weaknesses or improvements to the Bank's risk appetite assessment and/or enterprise risk framework to meet information management and information security best practice for the sector.
    d. Areas for improvement in the policies and procedures that the Digital Services and Information Security functions have implemented for the identification, management oversight, maintenance and assurance (Certification and Accreditation) of critical or high-risk information systems and/or end of life technology.

The Assessment covers the period from 20 December 2020 to 9 January 2021 being the period of the Bank's initial discovery and response.

The scope of the Assessment focused on the following key areas:

1. **Event timeline and actions**
    a. Obtaining and assessing relevant artefacts that support the initial and subsequent notification and communication of the vulnerability from the vendor, detection of the breach, implementation of the software updates and the decisions, actions taken prior to, during the incident and any immediate containment actions.
    b. Assessing the appropriateness and compliance with Bank policies on documentation/evidence supporting the process followed and formal approval of decisions made.
2. **Incident Response**
    a. Assessing the appropriateness of the incident response approach, governance, assessment of implications/risks and actions taken to mitigate/remediate the breach.
    b. Understanding the overall process followed and the level of alignment to the Bank's Incident Response Policies and Procedures and any other relevant external obligations.
    c. Evaluating potential areas for improvement in the Bank's current Incident Response Policies and Procedures.
3. **Risk Management**
    a. Evaluating relevant supporting documentation relating to the planned replacement of the at-risk file transfer system.
    b. Assessing the level of awareness of the potential risk exposure with the file transfer platform including the nature and extent of information stored, acceptable use requirements and guidelines, staff working practices and operational and security monitoring.

c. The level of awareness and action plans in place to address any relevant outstanding audit findings, recommendations and Post Incident Process Improvements (PPIs).

d. Any relevant perceived weaknesses or improvements to the Bank's risk appetite assessment and/or enterprise risk framework to meet information security and information management best practice.

4. Controls Assessment

The Assessment included an assessment of the design and operating (based on the level of risk) effectiveness of key controls designed to identify, prevent, detect, respond and recover from similar incidents in the future and their alignment with the Bank's risk appetite and enterprise risk framework and information security best practice. Key areas of focus will include:

a. *Information management:* Including the policies and procedures for classifying information assets, preventative and detective measures to detect data loss of high-risk information assets, information governance frameworks and polices in place, and staff awareness and training.

b. *Information Security Risk management:* Including logical access controls, monitoring controls, change control, software update and vulnerability management, and platform resilience.

c. *Platform management*: Including development and maintenance of an application inventory, ongoing risk assessment, systems ownership and roles and responsibilities, Certification and Accreditation processes and procedures during the application/system lifecycle, Platform maintenance and monitoring compliance with relevant standards of the Bank and Government requirements (e.g. NZISM).

d. *Governance*: Digital Services Risk management and reporting and KPIs, roles and responsibilities, budgeting and funding, strategy and roadmap development, governance reporting scope and regularity to the Bank's senior leadership team and the RBNZ board/Risk Committee.

Out of Scope

The scope excluded:

— Detailed assessment of the vendor control environment and software development processes and procedures.

— Attribution of any contributing factors to specific individuals involved in the incident.

— A comprehensive business wide review of information management practices, as the Bank is scheduling this for later in the year.

Summary of findings and recommendations

Background and Context

Unauthorised access was obtained to a third-party developed file transfer system, Accellion File Transfer Application (FTA) ("the System") used by the Bank in late 2020. This access was obtained by exploiting a previously unknown vulnerability in the FTA application.

According to a public report commissioned by Accellion from cybersecurity forensics company FireEye, the vulnerability was first exploited by a cybercriminal group on 16 December 2020. Since then, several further similar attacks have occurred at companies and government organisations worldwide. Security researchers indicated that the attack targeted known users of the FTA application.

The System was used by the Bank to share and store sensitive information, and some of that information is likely to have been obtained by an external threat actor.

Summary findings

The scope of our assessment focused primarily on the containment phase of the response up until 9 January 2021. Detailed analysis of what data was breached, and the subsequent actions undertaken, occurred after the period covered by our assessment and was subject to work performed by other independent parties engaged by the Bank.

The Bank's breach response continued for some months after 9 January and the Bank worked closely with domestic and international cyber security experts and other relevant authorities as part of the investigation and response to the attack. These activities were not in the scope of this assessment.

We noted that at the time of the breach the FTA solution was still supported by Accellion and the solution was at the end of its support life in April 2021.

The data breach was contained by the Bank and the required software update applied within 24 hours of being notified by the vendor on 6 January 2021.

While the direct cause of the incident (the zero-day vulnerability) could not have been predicted, there were several key contributing factors which directly impacted the scale and impact of the data breach:

- Software updates to address the issue were released by the vendor in December 2020 soon after it discovered the vulnerability. The email tool used by the vendor however failed to send the email notifications and consequently the Bank was not notified until 6 January 2021. At this time the Bank was also notified of the system generated alerts of potential anomalous behaviour. The software updates were deployed by the Bank on 7 January 2021 and investigations to confirm whether a breach occurred commenced.
- We have not sighted evidence that the vendor informed the Bank that the System vulnerability was being actively exploited at other customers. This information, if provided in a timely manner is highly likely to have significantly influenced key decisions that were being made by the Bank at the time. Having said this, the nature of the information provided in relation to the software update did indicate that the updates contained "critical, time-sensitive security fixes" which drove the immediacy of the Bank's response.
- Usage of the System by the Bank was not limited to secure file transfers as intended. Working practices evolved over time to the point where the System was also used as an information repository and collaboration tool, which was not in adherence with the Bank's 2014 guidelines on acceptable use of the System. Adherence would have significantly reduced the volume of information at risk.
- There were also initial alerts of potential malicious activity on the System in December 2020 that would have helped provide early detection had they been identified and/or followed up by the Bank's support staff. These alerts were default alerts enabled within the System since 2015.

There were also some key controls and working practices that were within the Bank's control that were not implemented, and/or existing controls that were ineffective which also directly impacted the scale and impact of the data breach:

- The System had not undergone a Certification and Accreditation ("C&A") process to understand and ensure that any key risks were identified and managed. The C&A process typically includes a Systems Risk Assessment and Controls Audit and would also document the classification of the information that is stored on the system along with the high-level security requirements and information protection priorities. This could have highlighted the risks with the Bank's usage of the System.

- Delays in the project to replace the System did not trigger any interim mitigating controls to be implemented or reinstated.
- The System Replacement Project required users to define use cases that represented current usage patterns. This however did not highlight any information security risks with the use of the System for file storage and collaboration.

The nature of the observations identified in relation to the Controls Assessment indicate that there are areas for improvement in the Bank's control environment. Improving the effectiveness of the highlighted control weaknesses will help ensure other security related incidents do not occur in the future.

Based on the Bank's publicly available Statement of Intent 2020-2023 and the 2020-2025 Funding Proposal, it is clear that the Bank already had some level of visibility of the potential underlying issues with its IT systems, including security, resilience and broadening other capabilities. We understand that a significant strategic modernisation program was already underway to address these issues.

In addition, during this Assessment we were made aware of several activities that the Bank had planned in response to the incident, some of which align with our recommendations. Our scope did not include assessing the design or operating effectiveness of these planned activities.

We noted the following key planned activities and workstreams which should help improve the overall control environment were focused on the following key areas:

- Review and formalisation of risk management activities around data/information management controls and the C&A process.
- Security alerting and monitoring processes.
- Various Digital Services and security projects to enhance and refine existing technical security controls to improve detective and preventative capabilities.

We wish to acknowledge that the Bank provided KPMG unrestricted access to staff and documentation required to complete this Assessment and accepted the findings from the Assessment in a positive manner. It was clear from the work we performed that the Bank has taken this incident very seriously and staff were forthcoming in identifying areas that required improvement.

Key Recommendations

We summarise below our findings and recommendations based on the agreed areas of scope.

Completeness and accuracy of the incident event timeline

Some key events in the timeline in the period up to 9 January 2021 were not recorded in the detailed incident log. The specific details have been provided to management separately. The likely cause of these gaps is that a scribe was not assigned to the Incident Response Team (IRT) until later in the response process.

The identified key events related to communications between the vendor and the Bank concerning the initial notification of the vulnerability and software updates to address the issue.

We were however able to correlate key dates noted in the Bank's incident log related to vendor notification of the vulnerability and software updates. The recorded timeline in the incident log used by the Bank for their external communications in relation to the event appeared to align with evidence we assessed.

It is not possible to determine the exact impact of these missing timeline events and if they would have materially impacted the overall timeline and outcome.

There were no other major discrepancies noted in the incident log.

Key recommendations 1.0

- *Consider conducting more frequent incident simulations to ensure key Bank staff and their delegates are familiar with all of the requirements of the Major Incident Response Plan, and adhere to the key requirements (or document the rationale for any deviations) such as maintaining a complete and accurate incident timeline.*
- *Update the detailed incident log accordingly.*

Incident Response Actions

From a process perspective, the Bank in general responded appropriately to the incident once it was detected and notified. A Major Incident Response Plan (MIRP) existed and was referred to during the event. The Incident Response Team (IRT) mobilised quickly despite having to call upon several delegated members due to the incident falling over the holiday period. Minutes and actions were recorded and later all key documentation was transferred to a restricted

location. Appropriate escalation to the Senior Leadership Team (SLT), key government security agencies and engagement of an external forensic security consultancy occurred in a timely manner.

We noted however that there was not strict adherence to all aspects of the MIRP with respect to the use of the defined playbooks and the initial assignment of the incident priority category.

It is difficult to extrapolate whether these factors would have materially impacted the overall timeline and outcome. In general terms however the IRT complied with all material aspects of the MIRP.

There were several other contributing factors and areas where improvements could have been made which would have limited the impact of the breach and the response times:

- There was a delay in searching for the alert emails of potential malicious activity once the vendor confirmed their existence and nature.
- As noted previously, we did not sight evidence that the vendor informed the Bank that the System vulnerability was being actively exploited at other customers. Timely access to this information is highly likely to have significantly influenced key decisions made by the Bank.
- Not all key Bank users of the System were involved in determining the extent of the potential breach as there was not widespread understanding of who was using the System, the nature of that usage and the at-risk information that was stored on the platform.
- Once the full extent of the issue was known, there was no evidence that the risk to other similar types of systems that could also potentially be at risk were considered. This may have identified additional precautionary detective and preventative measures. We note that the Bank did however consider other potential implications of the data breach.

Key recommendations 2.0

- *Review ongoing security training requirements for staff supporting critical systems based on the nature and type information stored and processed and the key users of the system or information.*
- *Review monitoring and alerting protocols for all key security and operational alerts to ensure there is appropriate escalation and a peer review/QA process to help ensure key incident information is not missed and the incident actions register is updated.*
- *Improve the continuous monitoring of the control environment for vulnerabilities, potential threats, and attacks by formalising a program of audits, risk assessments and user awareness of policies and procedures.*
- *Create a Digital Services On-Call & Overtime policy that aligns with the Bank's current requirements and clarifies staff roles and responsibilities.*

Risk Management

We noted the following that aligned with industry accepted practice:

- Where appropriate, the Bank leverages relevant All of Government (AoG) IT solutions, that have been certified by the lead agency and the Bank has assessed and implemented security controls according to the lead agency recommendations.
- The Bank has defined risk champions to support staff during the day to day risk management activities.
- The Bank's follows the Government Chief Digital Officer's (GCDO) risk assessment process and has defined and implemented risk governance groups to communicate enterprise risk across the key stakeholders.
- A formal C&A process exists that defines the relevant artefacts and assurance activities to be completed.

We noted several aspects of risk management and the control environment specifically related to the System and more broadly across the organisation that require improvement:

- The risk assessment process does not formally consider appropriate mitigation actions and approval processes when a project is delayed or when key risk decisions are made by the project teams.
- Acceptable use guidelines for critical systems are not regularly reviewed or communicated and enforced across the Bank.
- There is no consolidated register of the Bank's cyber risks and integration of the cyber risk framework with the enterprise risk framework.
- C&A requirements are not being consistently enforced and the exceptions process is informal.
- There is no policy/framework that provides guidance to users in scenarios where an external

party enforces use of its own file sharing tools/protocols.

- The Information Security Strategy/Roadmap or framework to ensure PSR/NZISM architecture compliance is not formalised.
- The System Replacement project did not appear to consider the requirements of the original 2014 acceptable use guidelines document or whether delays in the project should trigger any requirements for interim mitigating controls.

Key recommendations 3.0

- *Formalise the security strategy and roadmap and PSR/NZISM compliance architecture that is aligned with the Bank's risks and is endorsed by the SLT and the Board.*
- *Formalise the risk management process for C&A requirements and end of life platform exemptions and risk acceptance.*
- *Develop, enforce and monitor acceptable use guidelines and minimum security standards for all critical applications.*
- *Integrate the cyber and enterprise risk management frameworks to ensure consistent risk treatment and/or reduce gaps in risk identification*
- *Develop baseline standards for vendor communication protocols including requirements for maintaining/updating contact lists and agreed escalation protocols. These should form part of all vendor agreements.*
- *Develop a policy/guidance for users to cover situations where an external party may mandate its own file sharing tools/protocols that may conflict with Bank policies.*

Controls Assessment

Several of the expected key controls were in place including:

- Monitoring capabilities for potential malicious activity.
- A comprehensive set of information security policies exist that align with accepted practice and are generally fit for purpose.
- The bank is leveraging the security capabilities and the mature control environment available as part of the All of Government (AoG) Telecommunication as a Service (TaaS) offerings.

We did however note several key controls that were either missing or not designed or operating effectively. Some of these controls are fundamental to helping prevent other security related incidents occurring in the future.

There were several controls relating to operational security of the Bank's control environment which could be improved. Details of these findings and the associated recommendations have been provided to the Bank separately. We summarise below other key findings:

- The enterprise framework for data/information management, including a classification framework and policies and guidelines for the security of data in unstructured storage, is informal.
- Vendor and asset management does not operate under a formalised framework.
- A formal framework for third party risk management does not exist which would allow the Bank to identify and ensure it has appropriate controls in place to manage the risk.

Key recommendations 4.0

- *Develop a formal enterprise framework for data/information management that includes a formally approved enterprise wide classification standard.*
- *Establish clear policies and guidelines for the security of data in unstructured storage.*
- *Create a formal framework for vendor and asset management*
- *Define Platform and Information owner roles and responsibilities for support/on call and training/certification requirements.*
- *Develop a framework for third party risk Management that assesses the risk associated with all critical providers and defines controls that have been implemented.*

Recommended next steps

Addressing the findings and recommendations from this Assessment will help improve the Bank's overall security posture and help reduce the likelihood of a similar event occurring.

While many of the recommendations are technical in nature, it is important that a people and culture lens is also applied to the remediation program to ensure changes are properly embedded and sustainable.

To address the findings in this report a formal programme is required to ensure actions are tracked and monitored and that appropriate resourcing is allocated. Appropriate governance, resourcing and priority should be established to ensure the programme does not develop a siloed approach.

As the programme progresses the Bank should consider the benefits of ongoing independent checkpoints to ensure controls have been appropriately designed and are operating effectively. This will help provide confidence that remediation activities are appropriately addressing the underlying risks.

kpmg.com/nz