MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

# Briefing Note: Cybersecurity in the education sector

| | | | |
|---|---|---|---|
| **To:** | Hon Chris Hipkins, Minister of Education | | |
| **Date:** | 30 July 2021 | **Priority:** | High |
| **Security Level:** | In Confidence | **METIS No:** | 1267366 |
| **Drafter:** | Margaret-Anne Barnett, Ben Copsey | **DDI:** | 9(2)(a) [redacted] |
| **Key Contact:** | Mark Horgan | **DDI:** | [redacted] |
| **Messaging seen by Communications team:** | No | **Round Robin:** | No |

## Purpose of Report

To provide advice on the current state of cybersecurity across the education sector and agencies and the actions the Ministry of Education (the Ministry) and education agencies collectively could take to better protect the sector from cyber-attacks or service failures.

## Summary

- This request follows a recent education report on cybersecurity in schools and kura, and a rapid response on whether the Tertiary Education Commission (TEC) should be given a greater mandated role to help ensure providers of tertiary and vocational education are adequately protecting their digital systems, in light of recent events at Waikato District Health Board (DHB).

- You have asked for further joined-up advice from all the relevant agencies, as the rapid response did not convey the sense of urgency you hoped to see.

- There is a heightened awareness of the risks of cybersecurity threats in the education sector as the number and sophistication of cyberattacks continue to rise across all sectors. This report notes the education system is exposed to cybersecurity threats due to the education sectors' increased use of and dependency on internet connected IT system and services.

- Mitigating the risks is not straightforward. The education sector is devolved and diverse, governance arrangements and capabilities are different across the sector, even within the sub-sectors, and IT capability is widely variable.

- This leads to significant variability in the use of appropriate and reliable controls across education sector organisations and requires new approaches to respond to the rapid rise in the number and sophistication of cyber-attacks.

- The Ministry has in place a cyber security uplift programme and assists other education agencies where capability is stretched.

- The Education and Training Act 2020 provides for changes in regulations that could require early childhood services, schools, and Tertiary Education Institutions (TEIs) to ensure their IT systems and processes  meet specified cyber security standards. The same levers do not exist for Private Training Establishments (PTEs). Any regulatory change would require policy and legal consideration. There are a range of existing mechanisms such as the Education Digital and Data Board (EDDB), for a system wide response at an agency level.

- This paper has been developed in consultation with TEC and builds on the advice provided in the recent education report on cybersecurity in schools and kura [METIS 1262630], and proposes tactical interventions we will start, as well as a system-wide, longer-term action plan within a common approach to help mitigate cyber risks across the education sector and agencies.

## Recommendations

We recommend you:

1. **Note** the cyber work programme is underway in the schooling sector and that progress is accelerating

2. **Note** TEC in conjunction with NZQA is performing a risk assessment across universities, wānanga, ITPs (Te Pūkenga), Transitional ITOs (TITOs) and larger Private Training Establishments (PTEs)

3. **Note** that a holistic approach is required across the education sector, including early childhood, where an immediate assessment of the risk is required to align with similar assessments across schooling and tertiary

4. **Note** this briefing recommends the Education Digital and Data Board overseeing a coordinated approach to responding to cyber security across the education system

5. **Agree** to the Ministry working with education agencies to provide advice on the review of system settings across early learning, schooling and tertiary to clarify what is required for strengthened monitoring, assurance, threat and incident management, and recovery

   **[✓ Agree] / Disagree.**

6. **Note** that the TEC will provide you with the high level risk assessment by mid-August

7. **Note** we will provide you with further reports with advice on options, timeframes and resourcing, by the end of September 2021 as follows:
   a. System-wide settings required to strengthen monitoring, assurance, threat and incident management, and recovery together with any associated costs; and
   b. Integrated assessment and reporting of system-wide cyber uplift activities, threats, and status of incidents together with any associated costs

## Proactive Release

a **agree** that this briefing is not published at this time under the provisions of section 9 of the Official Information Act: Free and Frank Advice, section 9(2)(g)(i) and commercial sensitivity in relation to IT providers 9(2)(b)(ii).

**[✓ Agree] / Disagree.**

Zoe Griffiths
**Business Enablement and Support**

30/07/2021

Hon Chris Hipkins
**Minister of Education**

3/8/2021

## Background and Context

9(2)(k)

[redacted]

3. In the Ministry's report on TEC's 2020/21 Quarter 3 performance [METIS 1257554], we noted it had no role or oversight of cyber security, privacy and wider security, either directly or indirectly through its monitoring activities. You subsequently requested urgent advice on whether TEC should be given a greater mandated role in cybersecurity in light of recent events at Waikato DHB. We provided you a rapid response [METIS 1266840].

4. Measures required to mitigate cyber risks and respond to incidents in education will be significant and ongoing. The education sector is large and diverse, with early learning, schooling and tertiary providers serving around 1.5 million learners.

5. This paper discusses establishing a joined-up whole of education system response to cyber security, stewarded by the Ministry through the cross-agency Education Digital and Data Board (EDDB), delivered through coordinated agency response under a common approach and aligned with the New Zealand Cyber Security Strategy.[1]

6. Priority areas of the Strategy that need to be applied to the education system are:
    a. Resilient and responsive New Zealand
        i. supporting businesses, NGOs, community organisations, and individuals to be protected and resilient to major cyber incidents
        ii. improving the information security capabilities and resilience of the public sector.

7. Wider support for the Strategy within the education system will need to address:
    a. Building a strong and capable cyber security workforce and ecosystem
    b. Cyber security awareness within the education system and wider community.

## A brief assessment of the cyber security landscape and planned activities

### *Cyber Security Landscape in General*

8. The most significant threat to the New Zealand education sector that is likely to cause significant operational disruption is cyber criminals and specifically ransomware. The head of the United Kingdom National Cyber Security Centre speaking at the RUSI Annual Security Lecture on 14 June 2021 commented as follows:

[1] New Zealand's Cyber Security Strategy 2019 | Department of the Prime Minister and Cabinet (DPMC) https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019 page 8

> *"What I worry most about is the cumulative effect of a potential failure to manage cyber risk and the failure to take the threat of cyber criminality seriously. For the vast majority of UK citizens and businesses, and indeed for the vast majority of critical national infrastructure providers and government service providers, the primary threat is not state actors but cyber criminals, and in particular the threat of ransomware.*
>
> *This has become more evident than ever during covid – that we need to focus on victims not just threat, and that small harms can amount to a cumulative risk of national significance. This is the most insidious cyber security risk – not the threat from, but threat to; and not the loss of data but the impact on operations, large and small, that stops people and business from being able to live their day to day lives. The sheer volume makes it the most impactful threat we face. We have seen it affect the NHS with WannaCry, prevent students accessing classes in the last few weeks, and shut down local authorities at great cost to the public purse, meaning the public cannot access services, pay their bills or, in some cases, even buy a house."* [2]

*9.* The education sector is being impacted by global incidents that attract global media coverage such as the schools and the early learning service provider impacted by the Kaseya ransomware attack, and a school impacted by the attacks on Microsoft Exchange vulnerabilities earlier in 2021. The United States Federal Bureau of Investigation recently testified that *"the number of ransomware variants has grown; today, we have investigations into more than 100 variants, many of which have been used in multiple ransomware campaigns. Recently, we have seen "double extortion" ransomware – where actors encrypt, steal, and threaten to leak or sell victims' data – emerge as a leading tactic for cybercriminals, raising the stakes for victims, which in turn has increased the likelihood of ransom payments being made."* [3]

10. While much of the public focus and threat awareness is on large scale incidents that gain widespread media attention often due to the disruption to services caused, evidence overseas and domestically indicates that a range of other cyber security incidents will likely be occurring, affecting organisations operations and the availability, integrity and confidentiality of the information they manage, including student personal information.

9(2)(k)

[redacted]

12. Recent experience with the Waikato DHB cyber security incident, highlighted the complexity involved in supporting the DHB to restore services in light of a sustained outage and the flow on disruption to delivery of services in a similarly complex and integrated environment (both supply chain and dependency across common and integrated systems required to maintain operational continuity).

13. There are lessons to be learned for the education sector from this incident and from the follow-up actions and assessment of DHB cyber security preparedness across the country including working with the National Cyber Security Centre (NCSC) to lift capability. This includes work underway to modernise the Health Information Security Framework (HISF) and leveraging this experience to ensure our frameworks are similarly fit for purpose.

[2] Lindy Cameron speaking at the RUSI Annual Security Lecture - NCSC.GOV.UK https://www.ncsc.gov.uk/speech/rusi-lecture

[3] https://www.judiciary.senate.gov/imo/media/doc/Vorndran%20-%20Statement.pdf

14. The Ministry, with the support of the NCSC, is already working alongside affected organisations to restore services and we are continuing to improve our collective response over time.

### *Education Agencies*

15. The Ministry has a stewardship role across the education sector and monitors the Tertiary Education Commission (TEC), the New Zealand Qualifications Authority (NZQA), and Education New Zealand (ENZ). The entities are monitored quarterly, including against a recently developed Digital and Data Monitoring Framework that includes relevant national guidelines. These guidelines include the Protective Security Requirements (PSR), the New Zealand Information Security Manual, Privacy Act 2020, and will be updated to explicitly reference NCSC Guidance on a range of topics including cyber security governance, supply chain cyber security, incident management and other topics, plus CERT NZ guidance intended for broader audiences including individuals, businesses, and IT professionals.

16. The Treasury is responsible for monitoring Education Payroll Limited (EPL) and the Network for Learning (N4L). REANNZ is monitored by MBIE.

17. A cross-agency EDDB reports to the Secretary for Education as Chair of the Education System Governance Board and provides a forum for system level digital strategy and planning. This board is encouraging all education agencies to use the Digital and Data Monitoring Framework and is working on a refresh of the Education System Digital Strategy.

18. In late 2019 the Secretary of Education sought and received assurance from education agencies (including Crown companies and the New Zealand School Trustees Association) that they had plans in place to comply with guidance provided by the NCSC to manage and secure personally identifiable information.

19. The extent to which organisations have the capability, capacity, and funding to manage cybersecurity risk is proportionate to their size. While there is advice available to agencies, applying appropriate cyber protections can be onerous and require specialist expertise, making it challenging for smaller agencies to meet the NCSC guidelines.

20. The Ministry assists the small agencies where their capability is stretched. The agencies also share intelligence, for example, when the Ministry or N4L are made aware of a school cyber incident, they inform EPL, who then proactively monitor payment instructions from that school for any anomalies.

21. As part of the Ministry's Cyber Security Uplift Project, the Ministry has completed a review of all Ministry systems and applications, identified those that are not secure from a design perspective and is now strengthening the required enterprise controls. This work was initiated in response to the GCDO letter sent to all government agencies in October 2019, requesting that each agency review their IT security practices and:
    a. ensure that each agency is effectively managing information security risk;
    b. understand what mission-critical information and IT infrastructure needs to be protected;
    c. ensure that the systems and information is protected appropriately.

22. The Secure Controls Framework[4] (SCF) that has been used as the basis for the assessment helps ensure consistency across the multiple assessors and is an approach that can be leveraged across the sector.

23. We will work with Education agencies to strengthen cybersecurity management and monitoring and make cyber security a priority for the Education Digital and Data Board.

***The Tertiary Sector***

24. As is the case across the whole education sector, the risks in the tertiary sector vary according to the size and capability of tertiary education providers. The eight universities, Te Pūkenga and three wānanga have significant interest in information management and data security. Their respective research agendas also require them to protect their intellectual property. Specific guidance for research organisations has been published by the PSR team (NZ Security Intelligence Service) in conjunction with Science NZ and Universities NZ[5].

25. The TEC has strong relationships and on-going engagements with the larger TEOs including universities, ITPs (Te Pūkenga), Transitional ITOs and a number of larger PTEs. As part of these on-going engagements, the TEC is aware of the good IT capability that these organisations are investing in and maturing to ensure their operational integrity. Most of these organisations, given their size, have their own IT business units including cyber security functions. The TEC is also aware that many of these TEO are investing in specific cyber security strategies and enhancement roadmaps, with board/council oversight, to continue to drive cyber security maturity within their organisations. The TEC's monitoring function does not currently require TEC to formally assure this area of operational concern.

26. In response to the request from the Minister, the TEC in conjunction with its cybersecurity partner Aura has created a cybersecurity risk assessment aimed at those organisations it would expect to have formal cybersecurity practices in place. This includes universities, wānanga, ITPs (Te Pūkenga), Transitional ITOs (TITOs) and larger PTEs. These organisations account for over 90% of enrolled learners in the tertiary sector. They also have people in roles such as Chief Information Officers or equivalents that would understand and be able to answer the questions in the assessment.

27. The cybersecurity assessment for the universities, wānanga, ITPs (Te Pūkenga), TITOs and larger PTEs was sent on 29 July 2021, with a response requested by Wednesday 3 August. This date was chosen as it is unlikely TEC would get a meaningful and informative response if it only allowed a shorter period of time for these organisations to answer the assessment. In developing the questions, TEC tested them with some key sector Tertiary Education Organisations (TEOs). The timeline is:
    a. Responses to the assessment back Wednesday 4 August
    b. Analysis of responses completed by 6 August
    c. Identify any potential need for further risk mitigations by 11 August
    d. Develop and report findings by 11 August
    e. Further actions based on findings and need for follow up with TEOs.

28. A second phase of cybersecurity assessment is being planned. This phase will target smaller TEOs (about 375 organisations). Many of the smaller TEOs would struggle to answer the questions in the current assessment and as a consequence, the validity of

[4] A security "control" is a safeguard or countermeasure to avoid, detect, counteract, or minimise security risk. Each assessment used 54 security controls (questions) across 13 SCF domains.

[5] PSR-ResearchGuidancespreads-17Mar21.pdf (protectivesecurity.govt.nz) https://protectivesecurity.govt.nz//assets/Campaigns/PSR-ResearchGuidancespreads-17Mar21.pdf

any response would be compromised. Time is needed to develop a more guided approach to enable respondents to understand what TEC is seeking from them. The TEC is working with NZQA to undertake this phase in parallel with phase one of the cyber security assessment due to its relationship with PTEs.

29. The assessment of the tertiary sector has started and will be built upon, taking lessons from the health sector, the Ministry's internal assessment and the schooling sub-sector to obtain concrete information about where the risks lie and what actions may be required.

***Schooling Sector***

30. The Ministry is implementing immediate tactical actions (as set out in paragraphs one and two) to address cyber security risks in the compulsory schooling sector, whist also developing a framework for better supporting schools and kura with IT.

31. We are completing the early-stage design and requirements for the offline backup capabilities and the interim email protection capabilities for schools and kura. We have completed the technical design for a secure access to school networks and are starting to roll this out to schools and kura. We are currently assessing options for cyber security insurance for schools and kura and are creating and education and awareness campaign for cyber security.

32. Funding from the COVID-19 Response and Recovery Fund announced last year, has enabled the Ministry to work with N4L to improve cybersecurity support for schools through a Cybersecurity Operations Centre as part of the Te Mana Tūhono programme. The centre is using international best practice to help schools manage cyber threats by proactively checking network security settings, monitoring network traffic and internet facing services.

33. The next stage is to gather data from 400 schools, which have already entered the Te Mana Tūhono programme, through our new Security Monitoring Platform. This will help us improve our knowledge of cybersecurity issues in schools. We expect this to be completed in August.

34. The schools are aware they are receiving a level of cybersecurity support through the Te Mana Tūhono programme. School networks are seeing levels of improved security as they transit through Te Mana Tūhono's phases. N4L are sharing these benefits when they engage with schools as they enter the programme.

35. We will continue updating you on progress of these improvements

***Early Childhood Education***

36. There are more than 4,600 licensed early learning services in New Zealand, comprising a diverse mix of teacher-led and parent-led services. All licensed services are required to meet regulations and licensing criteria.

37. Approximately 4,100 early learning services use Student Management Systems which feed data into the Ministry's Early Learning Information system.

38. Services are vulnerable to attack as was shown recently when a Kindergarten Association was impacted by the Kaseya attack, interrupting services in many of the 104 kindergartens and home-based services in the Association.

39. The Ministry produces an Early Learning Bulletin | He Pānui Kōhungahunga which we use to provide immediate guidance to early learning services about how to better protect their data and digital systems. We will strengthen this messaging in alignment with the broader education and awareness activities as part of the coordinated approach.

40. We expect that there will be the similar risks that we have identified in the schooling sector, however, we need to do further work to more fully understand the risk profile across this sector. We will do this through a co-ordinated assessment to understand the actions required and any policy implications of any proposed change.

## A Proposed approach for an aligned Education System response to cyber security

41. A whole of education system response to cyber security is required, stewarded by the Ministry through the EDDB, delivered through coordinated agency response under a common approach focused on the prevention, detection, and correction of cyber related risk. This will leverage the approach we have identified for the compulsory schooling sector with sub-sector specific targeted responses.

42. Achieving this will require systematic change from the development of strategies and informing policy and regulation, through to assisting organisations. Annex 2 provides a description of the activities that require coordination under this common approach.

43. The common approach will support stewardship of the response, whilst enabling appropriate tailoring of responses to the risk profiles within each of the three key sectors, early learning services, compulsory and tertiary.

44. This approach will need to recognise the diverse needs of the sub-sectors, the levers that are available and enable the application of frameworks and provision of services that are appropriate to the needs of each sub-sector and the maturity and capability of the organisations within them.

45. If agreed, we will initiate planning and design of the actions required to bring effect to the framework described above, including likely costs to inform funding discussions.

46. This will include identification of priorities and phasing including identifying immediate actions to address critical areas of risk.

We will report back to you at the end of September.

## Immediate Response

47. Along with the actions we are already taking for schools and kura outlined in paragraphs 30-34, we will take the following actions to strengthen measures in education agencies, early learning services and the tertiary sector.

48. The Secretary for Education has communicated with Education System Governance Board about cybersecurity. She will also send a follow-up letter to education agencies (TEC, NZQA, ENZ, N4L, EPL, REANNZ and the Teachers Council) seeking their assurance that they have risk mitigations in place that meet relevant national guidelines.

49. We will amend the Digital and Data Monitoring Framework used to monitor TEC, NZQA and ENZ to require regular reporting against specific cybersecurity criteria. In addition, we will provide this to Treasury against which EPL and N4L can be monitored.

50. The EDDB will focus on improving cybersecurity risk mitigations in its work across all education agencies.

51. We will develop sector appropriate and audience specific education and awareness campaigns to lift the sector capability and we use existing channels to support providers to better protect themselves from cybersecurity attacks and data protection.

## Next Steps

52. Initiate a cyber security assessment of the Early Childhood Education sector and collate the information with the findings from the Tertiary Sector assessment, and insights from tactical actions in the schooling sector to provide a baseline view of capability and key areas of risk requiring action. ✓

53. Investigate options to extend the Ministry role with respect to responding to cyber security incidents affecting early childhood services – i.e. in a future Kaseya like incident early learning services will be formally in scope of the Ministry's sector cyber security major incident processes. ✓

54. Work with the Ministry of Health and the NCSC to incorporate approaches and lessons learned from the integrated response required for the Waikato DHB cyber security incident to inform the development of our coordinated approach. ✓

55. Convene the EDDB to focus on the cyber security response for the sector including a common view of emerging risk. ✓

56. If agreed, report back on:
    a. System-wide settings required to strengthen monitoring, assurance, threat and incident management, and recovery together with any associated costs; and ✓
    b. Integrated assessment and reporting of system-wide cyber uplift activities, threats, and status of incidents together with any associated costs. ✓

    This will include identification of priorities, responsibilities and phasing including identifying immediate actions to address critical areas of risk. ✓

## Annexes

| | |
|---|---|
| Annex 1: | Tertiary Sector Cyber Security Assessment |
| Annex 2: | Common Approach Activities |

# Tertiary Sector Cyber Security Assessment

## Introduction

The government is taking a much greater interest in cyber security risks, in particular those risks that could cause service interruption or loss of private data in the education sector. As a result of this interest the TEC has been asked to undertake an urgent cyber security risk assessment across the tertiary sector.

The assessment will be used for form a view of cyber security risks across the sector.

## The assessment

This assessment is being sent to Universities, Te Pūkenga, Wānanga, Transitional Industry Training Organisations and all Private Training Establishments registered with NZQA.

The assessment consists of nine questions and should not take more than 60 minutes to answer. We are aware that many of you will have strong practices in place and this will be reflected in the answers to the questions. We are not after extensive detail. For most questions we are only seeking a tick box answer. If there is further explanation you would like to add to your answer please add them in to the response.

## How we will use the information

Responses will be collated and a view of cyber security risks across the sector formed. Based on your responses we may need to seek additional information.

Information gathered through the assessment will only be shared in an aggregated form.

## Response timeframe

Could you please complete the assessment and return it the TEC by 5pm Friday 30 July.

Please send your completed assessment to your Relationship Advisor.

# Cybersecurity Assessment

**Organisation(s) you are answering this assessment for** ______________________

**Contact name and email address for any follow up questions** ______________________

1. Does your organisation have a formal and established Cybersecurity Risk Management process? If so, how do you then deal with cybersecurity threats and risks?

   Response:

2. Does your organisation have cybersecurity governance established?

   Yes ( )    No ( )

   If yes can you provide a high level overview of how this works?

3. Does your organisation discuss and report cyber risks with the board or council?

   Yes ( )    No ( )

   If Yes, what type of reports do you provide and how frequently is it discussed?

4. Does your organisation have formally established roles for Chief Information Security Officer, and/or IT Security Manager and/or Cybersecurity Manager? Or are these roles outsourced?

   Yes ( )    No ( )

   If Yes is it:  Internal ( )    Outsourced ( )

5. Does your organisation follow and/or measure yourself against a cybersecurity framework such as NIST, ISO27001 or NZISM?

   Yes ( )    No ( )

   If Yes could you please state which one:

   If No do you have any plans to adopt a framework?

6. Does your organisation engage in any independent security assessments such as Cybersecurity Audits or Penetration Testing?

   Yes ( )    No ( )

   If Yes, when was the last time this occurred?

7. Do you have a disaster recovery and business continuity plan associated with a cyber security events?

   Yes ( )    No ( )

When was this last reviewed?

When was this last trialled?

8. Does your organisation conduct regular awareness and education programmes on cyber security risks?

   Yes (  )        No (  )

9. Does your organisation have formal and ongoing investment in cyber security risk management?

   Yes (  )        No (  )

# Annex 2 – Coordinated Response Activities

The table that follows illustrates the range of activities that will need to be coordinated as part of the common approach. Note that even tactical responses will require concerted effort and funding. Hence, clear direction and prioritisation of resource against an agreed outcomes framework will be critical.

| **Value Chain** | **Description** | **Proposed Range of Coordinated Activities** |
|---|---|---|
| Strategy and Objectives | Ensuring clear priorities for organisations, the Ministry and our stakeholders. | • Education System Cyber Security Action Plan<br>• Co-design of Policy and Responses<br>• Assessment of Existing Capability and Risk<br>• Monitoring and Evaluation<br>• Manage Government Relationships |
| Plan and Design | Creating the operational policies and the rules to operate under. | • Planning and Implementation of Initiatives<br>• Leveraging existing regulatory tools.<br>• Developing Standards and Operational Policy appropriate to each sub-sector<br>• Resource Prioritisation to Risk<br>• Sector Governance and Oversight |
| Develop | Create cyber security services and products to be consumed by the agencies and providers, and incorporated in the configuration of their services. | • Frameworks and Guidelines<br>• Creating Services to be Consumed by Sector |
| Engage | Proactive education and outreach with an understanding of organisations and their needs to target communications, raise awareness and influence behaviours. | • Education and Awareness Campaigns<br>• Identification of Organisations Requiring Assistance<br>• Understanding Needs<br>• Manage Stakeholder Relationships |
| Serve | Supporting organisations to protect information, manage security and ensure operation continuity. | • Providing Standard Audit and Assurance Services (Direct or Indirect)<br>• Providing Common Tools and Services<br>• Accreditation of Education Providers, Agencies and Crown Bodies<br>• Operational Intelligence and Insights<br>• Incident Reporting<br>• Detecting Cyber Security Incidents<br>• Resourcing to Respond |
| Assist | Providing assistance to resolve complex and technical issues and recover from service outages. | • Responding to Enquiries and Supporting Resolution of Complex Cyber Issues<br>• Enforcement of Compliance with Regulations<br>• Business Continuity and Resilience<br>• Recovery from Significant Disruption |