



Education Report: Initial Advice on Cybersecurity in Schools and Kura

To:	Hon Chris Hipkins, Minister of Education		
Date:	25 June 2021	Priority:	Medium
Security Level:	In Confidence	METIS No:	1262630
Drafter:	Margaret-Anne Barnett	DDI:	9(2)(a)
Key Contact:	Stuart Wakefield	DDI:	
Messaging seen by Communications team:	No	Round Robin:	No

Purpose of Report

This report provides advice on the nature and extent of cyber threats faced by schools and kura, and initial advice on measures that could be implemented in the short, medium and long-term to mitigate the risks. This is the first of three proposed reports:

- 1) Te Rito and the deployment of sLSR
- 2) Options to address challenges in the SMS market
- 3) Options to implement a framework to better support schools' IT, which we will follow with a business case and possible bid for funding from Budget 2022/23 subject to your support.

Summary

- Cyber threats continue to rise steeply across all sectors. Schools and kura are an attractive target on account of the personal information they hold and particularly vulnerable because not all the systems they use are adequately protected.
- Schools' critical dependency on digital technologies for learning and day-to-day operations is growing steadily and has accelerated as a consequence of the Covid-19 pandemic, increasing the potential impact of cyber risks.
- There is support available to help protect schools and kura from cyber threats, particularly through N4L, but the risks are escalating rapidly and more needs to be done.
- Two areas are of particular concern – the foundational digital infrastructure in schools and kura, and the software they run that holds personal and/or sensitive data, such as student management systems (SMS) and learning management systems (LMS).

These elements of the school's digital environment are particularly vulnerable to attack or service failure if the necessary protections are not in place.

- As independent Crown Entities, schools and kura are largely responsible for managing their own digital environments. Schools' capacity and capability to manage risk is widely variable and in general below what is needed.
- There are no easy fixes. Implementing all the necessary mitigations to protect schools' digital environments will require changes in policy, significant investment over a number of years; and may have commercial implications for existing providers.
- But there are immediate actions we can take. This paper provides advice on possible short, medium and long term interventions to reduce cyber risks and seeks your agreement to the development of a comprehensive framework for better supporting schools and kura with IT.

Recommendations

We recommend you:

1. **Note** the wide range of presenting risks due to cyber threats and the potential impacts of these on all participants in the education system;

NOTED

2. **Note** that many schools, kura and key service providers lack the capability or capacity on their own to mitigate these threats, which continue to grow in number, sophistication and complexity;

NOTED

3. **Note** that while the Ministry and N4L provide a range of centrally funded cyber threat mitigations, these do not provide complete protection and are currently optional for schools;

NOTED

4. **Note** we intend to begin implementing the following immediate tactical responses, which we estimate will cost around \$6m in 2021/22. We hope to reprioritise this funding mainly from Primary and Secondary Education MCA baselines but this is still likely to require support from the Minister of Finance:

- (a) Establish offline backup capabilities for schools and kura
- (b) Establish interim email protection capabilities for schools and kura
- (c) Accelerate the rollout of secure access to school and kura networks
- (d) Review cybersecurity insurance arrangements
- (e) Run a cybersecurity awareness campaign;

NOTED

5. **Note** this paper also proposes a shift to centrally managing critical IT infrastructure and services on behalf of schools and kura, providing better support for IT and protecting schools and kura from cyber threat and digital service failure;

NOTED

6. **Agree** to the Ministry providing advice on a framework for better supporting schools and kura with IT as proposed in this paper. This would require investment, which subject to your support we would seek through a bid from Budget 2022/23;

AGREE / DISAGREE

7. **Note** we will provide you with further reports as follows:

- (a) By mid-August, advice on Te Rito and the deployment of the sLSR
- (b) By end of August, advice on the options to address challenges in the current SMS market, including security and privacy standards
- (c) By end of September 2021, subject to your agreement to rec 6), options on a framework for greater central support for IT in schools and kura, and
- (d) By end of February 2022 a business case to implement the framework, followed by a bid for funding from Budget 22/23.

NOTED

Proactive Release

8. **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).

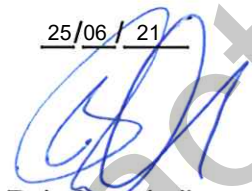
AGREE / DISAGREE



Zoe Griffiths

Business Enablement and Support

25/06/21



Rob Campbell

Education Infrastructure Services

25/6/21



Hon Chris Hipkins

Minister of Education

4/7/2021

I would like this work given an even greater sense of urgency than the paper suggests. We can't afford to lose a single day given the vulnerability. Schools do not have the capability or capacity to manage these issues and it is unfair to ask them to do so. We need to urgently provide more support from the centre. CH

Introduction

1. On 8 June 2021 you requested a briefing outlining cybersecurity risks and their impacts, following a strategy meeting to discuss the Te Rito project and issues raised about cybersecurity vulnerabilities. You asked for options to mitigate the risks, and in relation to Student Management Systems (SMS), you asked that we consider the sourcing environment, and associated impacts on the SMS and Learning Management System (LMS) markets.
2. While schools and kura can never be fully protected against cyber threats, there is much that can be done to reduce risk. Implementing more robust measures as described in this paper will take time and investment, but there are immediate actions we can take. This paper provides initial advice, structured as follows:

Part one: Cybersecurity in schools and kura

- The nature, likelihood and impacts of cybersecurity risk
- Vulnerability in a school or kura digital environment
- Student Management Systems

Part two: Approaches to address cybersecurity risks

- A framework for improving IT support to schools and kura
- Standards and accreditation
- Implications for the SMS & LMS market
- Implications for Te Rito and the Learning Support Register
- Wider implications for supporting schools and kura with IT
- Existing measures to mitigate risk
- Options to further mitigate risks

Appendix 1: A possible framework for supporting schools' and kura IT

Background and context

3. Schools and kura are largely responsible for their own IT, but their capability to protect their systems from cyber-attacks is highly variable. School boards must comply with a range of legislative requirements¹ relating to data and privacy, as well as detailed technical guidance on IT security from the relevant agencies. Many boards lack the capacity and capability necessary to meet these responsibilities, and can struggle to find specialist expertise, especially if their schools are small, rural or remote.
4. Many schools are likely to welcome greater support for IT. Reports by NZCER based on surveys of school principals indicate many principals find managing IT to be costly and burdensome².

¹ including, but not limited to, the Education and Training Act, Privacy Act, Public Records Act and Official Information Act.

² Primary Principals reported "Cost of purchasing, maintaining, and replacing digital devices & infrastructure" at the third highest 'major issues facing principals' schools, after "Too much being asked of schools", and "funding". [NZCER National Survey Primary 2019.pdf](#) page 163

Secondary Principals reported "Cost of maintenance and replacement of digital technology" as the 5th major issue facing principals' schools (55%) and "Dealing with inappropriate use of technology" as the 7th major issue. [NZCER Nat-Survey-Report-Secondary.pdf](#) page 144.

5. These issues are exacerbated by evidence of poor design and implementation of many of the applications schools rely on for their day-to-day operations. This is particularly acute with education sector specific applications such as SMS. Many vendors in this space are small local companies that do not meet standards typically required by government.
6. The adoption of cloud technologies, while mitigating many of the risks, is also exponentially increasing the number of software applications in use, due to their ease of access, flexibility and scalability, and in many cases the offer of 'free' versions. The increasing use of data driven learning insights and adaptive learning applications is vastly increasing the amount of student data being held in such systems, and many hold data offshore, not necessarily subject to NZ jurisdictional protections.
7. Support for cybersecurity is available to schools from the Ministry, Network for Learning, Netsafe, NZSTA and CERT NZ, and the Ministry continues to strengthen cybersecurity through Te Mana Tūhono programme. But the risk of cyber-attacks and data breaches continues to increase. For example, CERT NZ recently stated that malware attacks went up by 2008 percent in 2020 compared with 2019³.
8. A review of New Zealand and international evidence (in draft⁴) commissioned to inform the refresh of the Education System Digital Strategy found that the lack of a coherent, integrated approach to digital provision and use is one of the biggest barriers to the safe, secure and effective use of digital technologies in schools. The problems relating to IT in New Zealand's highly devolved education system extend beyond the threats of cyber-attacks and data breaches, posing risks to the day-to-day functioning of schools.
9. The escalating risks indicate a need to take a whole-of-system view and provide more comprehensive IT support to schools than is currently available, including stronger safeguards for student data and IT systems. As well as providing better cyber protection, supporting schools with foundational digital services could leverage economies of scale and free up schools to focus on teaching and learning.
10. Such an approach would require reconsidering how much choice schools exercise over the digital technologies they use. Appendix 1 describes where the boundaries of school choice could lie in future and indicates both the rationale for moving away from today's highly devolved approach, and the significant implications of such a shift.

Part One: Cybersecurity in schools and kura

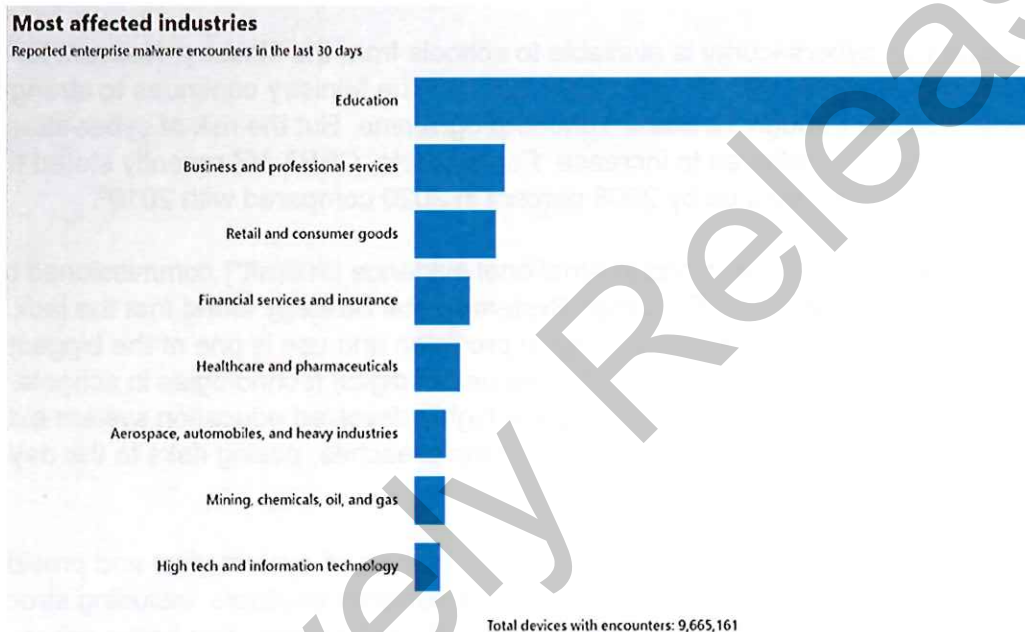
The nature, likelihood and impacts of cybersecurity risk

11. Schools are at risk of targeted and untargeted cyber-attacks. Schools are particularly vulnerable as many of the systems they use have not been engineered with security as a key requirement nor kept up to date as new cyber threats emerge.

³ Cited in an RNZ report of 14 June 2021: <https://www.rnz.co.nz/news/business/444660/dealing-with-cyber-criminals-some-nz-businesses-feel-they-have-no-choice-but-to-pay>

⁴ Evidence Review: Digital technologies in education during the COVID-19 pandemic, D. Wenmoth, June 2021 (In draft).

12. The rise in targeted attacks against education sectors worldwide seems primarily motivated by financial gain through extortion (via ransomware), where the loss of data and function has a high “real world” impact leading to higher ransom demands. The sector is particularly attractive from a criminal perspective as the personal data held can lead to identity theft, often as a pre-cursor to further criminal activity.
13. Untargeted attacks are mostly a consequence of poor security practices, such as weak passwords and unpatched devices, and the sheer volume of systems, devices and users involved. The graph below from Microsoft demonstrates the scale of the risks drawn from evidence of malware from 9.6 million devices. 63.6 percent of these malware attacks were devices used for education purposes.



[Cyberthreats, viruses, and malware - Microsoft Security Intelligence](#)

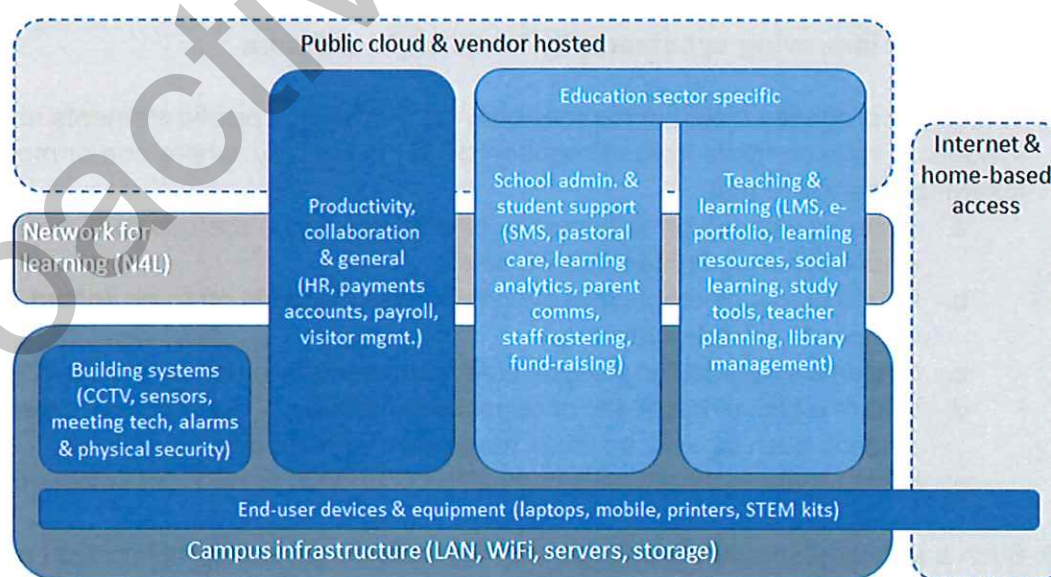
14. The education workforce is also an area of significant exposure to cyber risk through sophisticated social engineering attacks, often via “phishing” email. There have been numerous examples of this, typically resulting in users downloading malware or being duped into undertaking financial transactions on behalf of criminal actors.
15. As new cyber risks emerge, and the volume of attacks increase, the cost, complexity and sophistication of the required technical mitigations require significant upskilling of technical staff and those making risk decisions on behalf of a school or kura.
16. As there are no accreditation standards for school software or IT providers, there is no easy way for schools to assess the security or privacy aspects of digital products or services. This often leads to decisions based on function, cost or local availability.
17. While the move to cloud-based services may reduce some risks, it creates new ones, for example, multiple large multinationals, and at least one NZ cloud-based SMS vendor, have suffered significant privacy breaches. Even well secured solutions can be weakened by the way the tool is implemented or used (e.g., shared passwords, sharing of incorrect information or poor access control configuration).
18. School boards are responsible for managing these risks but it is challenging for schools to do so. There are changes in legislation (Privacy Act 2020, Education and

Training Act 2020) that must be factored into the decision making. While the information is readily available, and advice is provided by CertNZ, N4L, Netsafe, NZSTA and the Ministry⁵, many schools lack the capacity and capability to consume this information and act on it.

19. As a last line of defence in the event of cyber-attack, or any other event causing a system outage, schools need to undertake appropriate business continuity planning, which for cyber-attacks includes a backup of critical data. While this planning is often done well for natural disaster scenarios, as schools become more dependent on IT, their mitigations and plans for dealing with system outages have not been done so well. Schools must balance resilience and cyber protections against other cost pressures, which may lead to schools making risk/reward decisions based on limited knowledge of cyber risks.

Vulnerability in a school or kura digital environment

20. The diagram below describes the many elements that make up a school's digital environment. While each element is vulnerable to specific types of cyber-attack, the high level of interdependency and connectivity between them creates a compounding effect. This means a school's digital environment is only as strong as its weakest link. Conversely the highly devolved nature of the sector provides a degree of mitigation against a whole of system attack, i.e., while each school is vulnerable, it is less likely the whole of the education system can be attacked at once.
21. A literature review of learning from the Covid-19 pandemic (referenced on p.4) found that a lack of a coherent, whole-of-system approach to the digital environment is a significant barrier to the safe and effective use of digital technologies for learning. If each element is not appropriately protected the system is more exposed to cyber-attack, operational interruption, and data breaches. A whole-of-system, end-to-end approach to managing the digital environment is needed to protect against failure or attack.



Elements of a school's digital environment

⁵ [Protect your school from cyber-attacks and cybersecurity breaches – Education in New Zealand](#)

Student Management Systems

22. Student Management Systems (SMS) are part of a group of education sector specific applications used for school administration and student support that in New Zealand are typically tailored to NZ requirements.
23. As a result, this group of applications is dominated by small NZ vendors with limited resources, which has exacerbated the variable cyber-security maturity – a particular concern given the sensitive nature of the information held in these systems. Also, the recent commercial failure of the Assembly SMS (Schola) has raised the prospect that other SMS vendors may be financially vulnerable.
24. The SMS market is dominated by two vendors – at 1 March 2021, KAMAR had 16 per cent of all state and state integrated schools (84.4 percent of secondary schools), and eTAP 39 percent (48.6 percent of primary and intermediate schools).
25. SMS vendors are increasingly implementing learning management functionality (a global trend), and thus increasing the amount of student level data they hold, which reinforces the need for a comprehensive approach to any interventions.
26. SMS have significant differences in functionality, are typically deeply embedded in school operations, are integrated with a range of other school systems, and are difficult to change as they tend to determine key operational business processes. Fewer than 0.5% of state and state integrated schools have an SMS that is also used in other countries.
27. Part two of this paper proposes approaches to address cybersecurity risks in schools, including the centralised procurement of SMS and other higher risk education specific applications.

Part two: Approaches to address cybersecurity risks

A framework for improving cybersecurity for schools and kura

28. This paper proposes a shift in responsibility for managing specific elements of schools' IT environments from school boards to the Ministry, where one or more of the following criteria are met:
 - a. Systems with a high likelihood/impact of cyber risk, such as SMS software where sensitive student data is held
 - b. Foundational elements that everything else depends on to be secure, such as campus IT infrastructure
 - c. Systems essential for physical safety and security, such as alarms & CCTV
 - d. Where a lack of capability or capacity to manage IT and mitigate cyber risk is evident, such as in IT services provision in remote and rural areas
 - e. Where there is otherwise a compelling economic or operational benefit.
29. Such a shift would require a change in policy settings, including limiting the choice school boards currently exercise over the procurement and management of IT services. To implement this approach further policy work would be required to determine whether schools could opt-out and if so under what conditions (e.g. by attesting that their IT environments meet the prescribed interoperability, security and privacy standards). For services the Ministry provides today the settings are opt-in

rather than opt-out, apart from the cyber insurance cover provided as part of school contents insurance.

30. The following approach would see a shift from the current highly devolved system to one in which IT services at greatest risk of attack or failure are centrally procured and managed. A range of digital services could be centrally delivered in much the same way as network services are delivered by N4L. The level of choice schools exercise would depend on the nature of the services they require, the degree of risk inherent in each, and the school's capability to manage their own IT.

A possible approach to support schools and kura manage their digital environments

Centrally provided	Managed choice	Local choice
The Ministry procures, funds and centrally manages specified core IT services, which all schools use, to the standard expected of government agencies	Schools select from a limited range of services procured on behalf of schools by the Ministry that meet a high threshold of capabilities and standards	Schools can select from a catalogue of services that meet a minimum threshold of required capabilities and standards
Underpinned by a comprehensive standards and accreditation regime		

31. This approach is set out in more detail in Appendix 1, showing the range of technologies and digital services that could fit under each category.
32. Taking the approach suggested above would have significant benefits beyond providing protection against cyber threats. When common standards are applied across digital services, schools can collaborate easily with others, share data more safely, and save time and money they would otherwise spend on managing their own systems.

Standards and Accreditation

33. Accreditation or assurance of required standards is fundamental to give education sector participants, including ākonga, parents & whānau, confidence that the technology they use and their data are appropriately secure. We propose an assurance regime to underpin all school IT systems, based on agreed privacy, security and interoperability standards that are fit for purpose for the education sector.
34. Various Australian State governments, in conjunction with the federal entity Education Services Australia, have been trialling a shared service for such purposes under the brand "Safer Technology for Schools" (ST4S). This service assesses and accredits any technology used in schools against the aggregate of state and federal security & privacy requirements and provides a published assessment of the results.
35. We have engaged with Education Services Australia on the possibility of NZ joining this scheme given the high levels of compatibility of security and privacy requirements. Such a shared arrangement would expedite the process, reduce its overall cost, and ensure vendors who are common to both jurisdictions need only complete the process once.
36. The option for NZ to join the ST4S scheme is still under consideration by Education Services Australia and we are expecting a decision on whether this will be an option before the end of 2021. In the meantime, we have secured agreement for Te Rito to leverage the scheme as part of its assessment of SMS vendor security and privacy capabilities.

Implications for the SMS & LMS market

37. As part of the framework above, SMS, LMS and other higher risk systems containing student data would be provided under a "Managed Choice" scheme, with schools able to select from a limited set of centrally procured (but not necessarily centrally funded) options. This approach could include resetting the contractual arrangements for education software, with the Ministry procuring vendors directly on behalf of schools.
38. In evaluating the functionality of current SMS products, it is apparent the market has differentiated between the needs of, for example, a large secondary school versus a small primary, with many more features available to support the more complex needs of larger secondary schools. For this reason, it may not be sensible to consolidate to a single SMS for the whole system, but rather a smaller selection of products to ensure there is a secure, accredited product in each segment of the market.
39. LMS products are not universally used across all schools and kura, as evidenced by the need to provide a temporary LMS solution to a large number of schools during the COVID lockdown period. There are potential benefits that could be derived from closer integration of LMS with the planned new Online Curriculum Hub (OCH). Further analysis of the LMS market and exploration of the linkages to OCH will help inform the benefits of having either a single LMS or multiple LMS products across the system.

Implications for Te Rito and the Learning Support register

40. The Ministry has a high threshold for systems to connect to Te Rito, including an internationally recognised specification that lays out the standards that SMS providers integrating with Te Rito must meet. In addition, the data populated within Te Rito provides a secure back-up of core SMS data, aiding recovery in case of a breach that impacts a specific school or SMS provider.
41. Te Rito requires 2-way data exchange with a school's SMS to support its various intended functions, including the sLSR. This was envisaged to occur through a direct interface to ensure data is always up to date and avoid placing additional workload on the education workforce.
42. As a result of identified security weaknesses in the school IT environment affecting integration with school SMSs, and in some cases the SMS products themselves, the national deployment of Te Rito is unlikely to be viable across all SMS products until such time as the interventions noted in this paper can be effected. This means the current rollout is effectively paused for the foreseeable future. Further deployment will be considered as and when we are assured that the integrations between SMS vendors and Te Rito meet the necessary standards.
43. We are actively exploring other options for the deployment of the Learning Support Register, that will balance the opportunity to deliver value to the sector with longer term strategic alignment with Te Rito. This includes the benefits and implications for schools, how data integrity will be maintained, security and privacy, technical complexity and risk. We will report back to you on options and a recommended approach in mid-August.

Wider implications for supporting schools and kura with IT

Governance

44. A simplified framework covering IT Governance, Security and Privacy targeted at schools and their common operating practices is likely to be required to enable schools to assess their governance practices and secure use of IT efficiently. This could be similar to the Health Information Security Framework produced by the Ministry of Health to support the Health and Disability sector.

Balancing Innovation and Risk

45. Implementing a system wide, end-to-end approach to schools' IT need not limit innovation; on the contrary, common interoperability, privacy and security standards could facilitate innovation by making it easier for schools to collaborate with others and share data securely.

Bring your own device policies (BYOD)

46. BYOD policies are implemented by many schools but are not addressed directly in this paper. Our position is that schools are best placed to determine their own device policies. Personally owned devices can be a vector for malware, but applying the necessary protections requires negotiation with the owner of the device. Compensating controls can help mitigate but not eliminate these risks.

Existing measures to mitigate risks

47. The approach to supporting schools' IT described above, while helping ensure all schools are equipped with robust, secure IT, would require significant changes to the way the schools' system operates and take considerable time and investment to implement.
48. There are short term measures that would go some way to reducing risk. The section below provides advice on what is already in place, in progress or planned, and that could be implemented in the next one to two years subject to funding.

Building on existing measures

49. Each year N4L is allocated \$28.7m for the Managed Network; and through Te Mana Tūhono, \$68.7m is allocated to hardware replacement and the establishment of a Security Operations Centre. The Ministry funds Netsafe at \$812,000 per year to support schools and kura with online safety.

Extend existing capability

50. N4L's managed network service for schools provides traditional network centric security controls to schools including firewalls, content filtering and secure remote access. A small number of schools still opt-out of N4L's firewall service in favour of their own solution. This creates an unknown level of risk and avoidable additional cost for those schools.

51. Cybersecurity insurance cover to help schools recover from cyber-attacks is included in the Ministry's risk management scheme (RMS) for schools and used by around 50% of schools. The balance of schools may have independent cybersecurity insurance but no record of this is kept. We intend to undertake a review of policies, including the position on ransomware payment, and coverage of non-RMS schools.

Expedite in-progress activity

52. Negotiations are underway to renew existing Google and Microsoft agreements (expiring Dec 2021) to expand the range of products available to schools within the existing funding. This will include an expanded range of security products, including email protection, scaled over three years for a limited number of schools. This could be expanded further subject to available funding for both licensing and deployment.
53. Through the Te Mana Tūhono programme the Ministry is standardising schools' internal IT network management and network equipment, including implementing network security controls within each school's IT network. This work is scheduled to take place over the next three years in line with the end-of-life dates for existing equipment but could be expedited to bring forward the security benefits, subject to available funding, and writing off older, less secure equipment.
54. N4L is establishing a Security Operations Centre (SOC) to support schools and kura through the proactive monitoring of cyber threats across the various elements of schools' IT. The initial focus of this is on the IT network components of the infrastructure domain where N4L has an existing mandate with schools to detect cybersecurity incidents. We could extend the monitoring capability of the SOC beyond the initial network scope, subject to available funding

Additional Measures

55. Given the rising cybersecurity threats, we will take the immediate tactical actions 1-5 in paragraph 57 below, using reprioritised funding from Primary and Secondary appropriations.
56. In addition, we will prepare more comprehensive advice on how to better support schools with cybersecurity. This would include (but not be limited to) the list of actions 6-10 in the table below.
57. Providing appropriate IT support in today's IT environment will require significant investment in funding and expertise. We expect to need new funding which we would seek from Budget 2022/23, subject to your support in principle for the approach set out in this paper. Our advice would include an assessment of potential risks and liabilities to the Ministry that could result from a more centralised approach to IT procurement and management.

Action	Purpose	Estimated funding required
Immediate, tactical actions		
1 Establish offline backup capabilities for schools	To help schools recover from IT security and availability incidents.	\$1.1m to \$1.9m (depending on uptake) in FY2021/22 plus

		further costs in subsequent years
2. Establish interim email protection capabilities for schools	To help prevent and detect phishing attacks on schools and provide visibility.	\$1.5m in FY2021/22 plus further costs in subsequent years
3. Accelerate the rollout of secure access to school networks	Mitigate some of the risks from BYOD devices connecting to insecure school internal networks.	\$2.0M in FY21/22 plus further costs in subsequent years
4. Review cybersecurity insurance arrangements	To assess if cybersecurity insurance arrangements are fit for purpose for the risks facing schools.	\$100k in FY21/22
5. Run a Cybersecurity Awareness Campaign	Help increase cybersecurity awareness of school principals, boards, staff, and IT suppliers, potentially facilitated by N4L and in partnership with other key players (NZSTA, CERTNZ, Netsafe).	\$500k in FY21/22
Medium to long term actions (Indicative only)		
6. Develop accreditation frameworks for IT software and service	Enable the accreditation of IT software and service for schools to building on work already undertaken with Australian State Departments of Education (ST4S)	Advice on funding required will be included in a paper providing more detailed advice on a framework of support for schools' IT.
7. Strengthen management of TELA laptops for targeted schools	Provide support to ensure 8000 TELA Windows devices are receive monthly operating system and core application updates including security patches. This would be targeted at schools that do not already actively manage their TELA devices.	
8. Develop secure configurations for Google Workspace for Education and Office 365 for Education for NZ Schools	While some of this work is underway, we need to ensure that schools and IT providers have clear guidance on how to secure these platforms. To be developed in partnership with each vendor and with appropriate co-design with schools and other stakeholders / peak bodies.	
9. Develop a Schools IT blueprint to guide the investment and operation of Schools IT.	This would provide the overall framework for schools' IT upon which all the other interventions can be based. This would also include the design of a fit for purpose Cybersecurity standards framework defining minimum standards to be applied by schools or IT providers.	
10. Improve System Level Situational Awareness	To help the schools and Ministry catalogue the current delivery of schools' IT infrastructure and services to allow better understanding of system-wide risks and development future services and protection.	

Other avenues to explore outside of the Ministry's remit

58. The Education Review Office could potentially include a review of school boards' cybersecurity and data privacy practices as part of their regular review of schools.
59. Relevant agencies, such as GCSB and the Ministry of Justice, could consider the legal basis for prohibiting the payment of ransoms originating from cyber-attack thus reducing the attractiveness of NZ relative to other jurisdictions. Relevant agencies could also consider the interface between unregulated and untraceable cryptocurrencies (eg BitCoin) and the regulated monetary system to make it more difficult for criminals to realise value from cyber-crime.

Appendix 1: A possible framework for supporting schools' IT

(Draft only – not government policy)

