WAIKATO DISTRICT HEALTH BOARD (WDHB) INCIDENT RESPONSE ANALYSIS

Final Report 2 September 2022

INPHYSEC

Version v0.5

CONFIDENTIAL INFORMATION

Contents

1 INTRODUCTION

This is the final report on the 2021 cyber-attack upon the Waikato DHB (WDHB), prepared for the Ministry of Health. It is a summary of the information gathered for the Ministry of Health on lessons learned from the 2021 ransomware attack on the WDHB. This final report sets out our findings based on interviews and documentation received, and our conclusions and recommendations based on these findings.

This report has been prepared based on documentation we have reviewed from both the WDHB and the Ministry of Health. We supported this by speaking to many of the senior people in the WDHB, and the Ministry of Health. We have also had conversations with the National Cyber Security Centre (NCSC), NZ Police, local MPs, 9(2)(c), 9(2)(k) and other parties who were involved with the WDHB at the time of the attack. These conclusions have been shared with both the WDHB's then Commissioner and CEO, and the Ministry.

This is a complicated report, and a word of explanation is in order. Our Terms of Reference are appended to the report.

First, structure. The report covers some distinct phases in relation to the WDHB ransomware attack:

> 'Readiness' – the extent to which the DHB's online security was as strong as we would recommend. It is important here to separate the incident narrative from the descriptive: we have identified and set out a number of general issues (and accompanying recommendations). But only one 9(2)(k), 9(2)(c) was directly relevant to the progress of the 2021 attack;
>
> 'Response': what the DHB and others did when and after the incident occurred. Here, we try to provide order, structure, and explanation for a fluid, evolving situation. The judgements are hindsight ones, necessarily. At the time, none of the participants had full knowledge of the situation; all (so far as we can see) did their very best. This is an opportunity to learn lessons for the future, not to engage in retrospective, and unproductive blame.
>
> 'Recovery and restoration': putting systems back online. As you will read, this was complicated and controversial. It's the area that highlights the central trade-off between security and functionality. It's the area where some real policy choices lie ahead for Te Whatu Ora.

Secondly, scale. Some of what follows deals with the whole WDHB; other material deals with the detail of the configuration of the WDHB's IT systems, and the conduct of the attacker. This could be confusing, or distracting. We have considered dividing the report into two parts – general and technical. But we have concluded that this would not aid the reader – the reality is that incidents like this affect the whole organisation but can at times require a focus on points of technical detail.

2 BACKGROUND

On the 18 h of May 2021, the WDHB became the victim of a large-scale criminal ransomware attack. WDHB's initial response was to physically disconnect from the Internet and other health systems all its own services, including corporate IT systems, laptops, printers, phones, medical devices, and any cloud services to protect from any further potential compromise by the attacker. This affected healthcare services across the region, including Waikato Hospital, Thames Hospital, Te Kuiti Hospital, Tokoroa Hospital, and Taumarunui Hospital. It also affected other DHBs, primary and community providers who used shared services, including shared clinical services. Cloud services such as MS Teams, email, and the IT service management system remained available, and came to be accessed by clinical staff using 'new' machines.

As a result, surgeries were postponed, and seriously ill patients had to be transferred to other hospitals within other DHBs . Corporate and patient information was also posted on the internet and then reported in mainstream media.

Following the attack there was a significant amount of local and international media interest, with reports claiming that the attack was conducted using 9(2)(c), 9(2)(k) ransomware and that a large ransom was demanded.

It took several months for WDHB to restore the systems compromised by the attacker and address the backlog of surgeries and appointments that resulted from the attack. The incident was officially closed out on the 10 h of November 2021 – the majority of systems had been recovered and were operating securely by this date.

The Ministry of Health engaged InPhySec to complete a review to provide advice to the Minister of Health, the Chief Executive of WDHB, and the Ministry on what can be learnt from the ransomware attack and provide advice to help prevent or deal with subsequent attacks upon health systems. This includes assessing and evaluating the following areas:

- WDHB's risk assessment and controls prior to the breach to help identify cyber resilience vulnerabilities the WDHB had prior to the breach that can be mitigated in other DHB health and disability systems to strengthen the resilience of the sector.
- WDHB IT service restoration:
    - Governance and decision making
    - Timeliness
    - Awareness of risk
    - Expert assistance

3 APPROACH

The approach InPhySec used in the review followed an industry standard approach to such a review. This included constructing a timeline of events, and then (having reviewed

documentary material) exploring the experiences of participants through interviews. This process was used to draw out provisional conclusions, which were then discussed with participants.

By taking all the information gathered through documents received and the many stakeholders that were impacted by the attack, we were able to understand the nuances of the attack, the response, and its consequences which we have summarised in this report. The process was open, and collaborative with an aim to having participants speak freely and candidly about the attack and their experiences relating to it.

In preparing our report we have been mindful that fit for purpose security settings, procedures and processes - external and internal – are a critical responsibility under the Privacy Act 2020 of any agency that collects, uses, stores, and shares personally identifiable information (PII). Information Privacy Principle 5 states that organisations must ensure there are safeguards in place that are 'reasonable in the circumstances to prevent loss, misuse or disclosure of personal information'. We are not a regulator, but we have sought to ensure that our conclusions and especially our recommendations would tend reasonably to operate in a manner that would be consistent with that Act's provisions. We think the public interest demands no less. And, as will be seen, that balance between security and thus privacy on the one hand, and effective clinical services on the other turns out to be a central question in this case.

4 CONTEXT

There are three relevant components to the context for our review:

a) The global rise of a sophisticated, criminal ransomware economic and technical ecosystem from which New Zealand is not immune;

b) The journey WDHB had been on in recent years, which meant the DHB had a demanding agenda of necessary change and reform to tackle, across its entire scope of activity. It is commonplace that public health systems in many countries have been facing structural staffing and resource challenges in recent years, and WDHB was no exception to this underlying strain; and

c) The current transformation of the management of the healthcare system, through the merger earlier this year of the DHBs into Te Whatu Ora. This is a factor in the conclusions and recommendations we draw, as they need to be prospective of the new world if they are to be useful.

We take these in turn.

4.1 Global Rise of Ransomware

Globally, the number and severity of cyber-attacks has been increasing year on year with no sign of slowing down. Previously, an attack of the magnitude seen at WDHB would

perhaps have been attributed to advanced threat actors such as Nation States. However, the increasing availability of sophisticated tools, often available 'as a service' has led to this type of attack being dominated by criminal gangs.

The motive behind many cyber-criminal groups is primarily financial gain, but can also include peer recognition, and (sometimes) political gain. Whatever the motive, cyber-crime is booming, and many more organisations are finding themselves victims.

This is certainly true for New Zealand organisations. According to CERT NZ's *Quarter Three Report for 2021*[2] there was a 53% increase in incidents reported to CERT NZ between Q2 and Q3 of 2021. Noting of course, that this only counts incidents that were reported.

The same period saw some other notable ransomware attacks:

- The Health Service Executive attack[3] on the Irish healthcare system also in May 2021; and
- the Kaseya VSA ransomware attack in June 2021 that impacted ~1500 organisations.[4]
- As we finalised our report, a ransomware attack on a software provider supporting the NHS in England & Wales was reported, with significant disruption.

Cyber-attacks in the health sector have been progressively getting bigger over the last few years. In March 2021 Eastern Health, a major provider of health services in Melbourne, Australia experienced a similar ransomware event. We should also remember that in 2017 the NHS in England & Wales experienced a major cyber-attack (part of the WannaCry incident) that took 200 hospitals offline. That incident resulted in a major programme of cyber security improvement including the creation of a centralised NHS Security Operations Centre to detect and respond to major threats.

4.2 WDHB's Journey

Although it is strictly speaking out of scope, it is only right and fair to those involved to note that the WDHB had faced significant re-organisation and a demanding agenda of organisational and staffing change in the years running up to the 2021 incident. The Board itself had been set aside and its work placed in Commission by the Crown. In addition to the profound governance issues this implied, staff changes within WDHB meant many people were relatively new in their posts (from the CEO down), and the whole organisation was coping with a significant, demanding operational programme. On top of that, the Covid 19 pandemic had placed every health system under real pressure. These challenges were demanding and at times preoccupying for all involved. In these circumstances, it is noteworthy that the impact of the ransomware attack on patient delivery was significantly less than might have been the case. A different worst-case scenario could've seen the

Cyber-attacks conducted by a particular country in an attempt to further that country's interests.

[2] https://www.cert.govt.nz/about/quarterly-report/quarter-three-report-2021/

[3] https://www.bbc.com/news/world-europe-58413448

[4] https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/

clinical network also infected, a much more significant data breach or compromised backups. However, because WDHB's backups were provided by a third party and not accessible to WDHB, restoration via backup was always feasible, and so these potentially dire outcomes were avoided. Any of these alternative scenarios would have had an even more drastic effect on the patient experience at WDHB. That is not to downplay the severity of the effects as they were, even if they may have been less immediately obvious to patients due to the reduced capacity the hospital was running at due to the pandemic.

The COVID-19 story deserves a special mention. WDHB told us that the rapid changes made to support remote working as well as the need to adapt and respond to the pandemic was material to the state of IT systems at the time of the attack. They explained that the hospital IT environment went rapidly from having been designed to operate in a risk context largely limited to the physical location of the hospital(s) with fragmented and minimal digital access beyond those physical environments, to one where they were forced to rapidly adopt hybrid ways of working and new technologies, with a consequent escalation of risks arising from greater remote access. That said, Covid-19 was only one contributing factor in the state of WDHB's IT environment. It had grown organically in many areas to meet emerging needs for years. For its part, the Ministry told us that it had told all DHBs of the security risks of a large scale move to remote working in the Covid-19 context (drawing on advice from NCSC). This came in the form of an advisory of Covid-specific cybersecurity threats which included ransomware targeting healthcare.

It also became clear to us and was reflected in the DHB's own planning material during the incident, that health systems were more networked and more dependent on data exchanges than had been consciously realised. The health data ecosystem has evolved, as an emergent network over many years. This process has been largely clinician-driven, in many cases without the knowledge of IT teams. This has implications for how risk and security was approached and managed, and how it should be considered in the future. It will be a foundational challenge for Te Whatu Ora to identify and secure its digital assets when the evolution and use of those assets is both highly distributed and in a constant state of change.

4.3 Te Whatu Ora and the replacement of the DHB Structure

From 1 July 2022, the DHB structure in New Zealand is being replaced by a unitary health delivery entity, Te Whatu Ora. This will, over time, lead to a significant merger of DHB IT systems. In the meantime, the existing WDHB-origin arrangements and systems will continue. This is not relevant to the 2021 incident at WDHB, but it is highly relevant to our conclusions and recommendations as they affect Te Whatu Ora in the future. We have concluded that, whatever its eventual destination, we should frame recommendations against a system which will come to be managed in a centralised manner, nationally, with the ability to brigade resources across the whole health system, even if the underlying IT systems are a hybrid of national and older legacy DHB-origin systems for some time.

We also note the increasing connectedness of medical devices and tools to the Internet, the increasing ubiquity of mobile devices in medicine, and the need to provide for staff in the health system who will have complex patterns of work, often involving (from an IT

perspective) their own devices. These are trends to be accommodated so far as safely possible or otherwise controlled.

5 RANSOMWARE IN DETAIL

Before turning to the incident, a word on ransomware: CERT NZ defines ransomware as 'a type of malicious software that denies someone access to their files or computer system unless they pay a ransom'.[5]

The purpose of ransomware is to coerce a victim to pay a ransom, typically in cryptocurrency, to the threat actor so that the victim can regain access to their files and systems. In practice, even if a ransom were paid, the nature of proprietary systems as used by the DHB means there is a limited or nil ability to actually recover these systems.

According to Group-IB's report *Ransomware Uncovered 2020/2021*[6] the primary vectors of compromise for ransomware threat actors are external remote services (52%), phishing (29%) and exploitation of public-facing applications (17%).

Once a threat actor has obtained initial access, they will usually attempt to escalate their privileges by obtaining access to administrator accounts and begin to move laterally within the victim's environment performing internal reconnaissance to identify critical assets.

Through this, they will also access additional compromised credentials and systems, and embed themselves further into the environment seeking to remain undetected. With these compromised credentials it is possible for the threat actor to then remain in the network for several months or longer.

Following this the threat actor will look to delete or encrypt backups, obtain and exfiltrate copies of sensitive data and encrypt files, placing them in a better position to demand the ransom.

[5] https://www.cert.govt.nz/business/common-threats/ransomware/
[6] https://www.group-ib.com/resources/threat-research/ransomware-2021.html

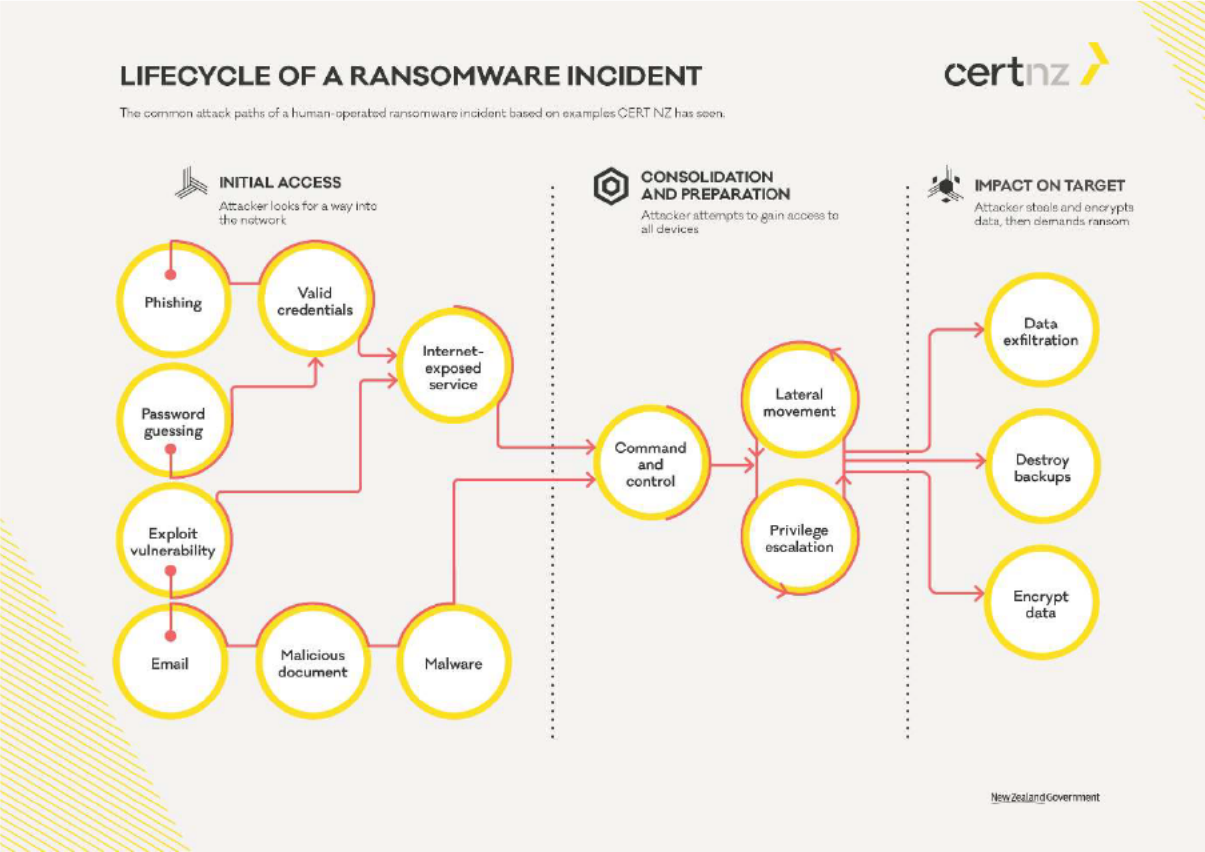


Figure 1: Lifecycle of a Ransomware Incident (Source: CERTNZ)

5.1 9(2)(k), 9(2)(c) Ransomware and 9(2)(k), 9(2)(c)

While attribution is always problematic, 9(2)(k), 9(2)(c) ransomware has been identified as the variant used in the WDHB attack. 9(2)(k), 9(2)(c) [redacted]

9(2)(k), 9(2)(c) is a ransomware-as-service (RaaS) product. 9(2)(k), 9(2)(c) [redacted]

RaaS allows threat actors to buy or lease ransomware found on the dark web, allowing groups with limited in-house technical ability to use more complex malware. 9(2)(k), 9(2)(c) [redacted]

9(2)(k), 9(2)(c) [redacted]

9(2)(k), 9(2)(c) [redacted] this means it is often used without a group claiming credit through their official channels. Therefore, it can be hard to pin what group has executed an attack. 9(2)(k), 9(2 [redacted]

According to Group-IB's report *Ransomware Uncovered 2020/2021*[8] the majority of ransomware attacks (64%) are as a result of RaaS transactions. This reflects the complex criminal 'ecosystem' that has evolved in recent years: all the benefits of specialisation, scale, 'as a service' provision, bulk data, and associated analytics that we see in the legitimate economy are used by criminal enterprises. As a result, they are efficient, operate at scale, are very innovative, and sophisticated. We underestimate them at our peril.

5.2 The Irish Healthcare System Attack

We have looked closely at the ransomware attack suffered by the Irish Healthcare system in May 2021. The Irish Healthcare system (called the Healthcare Services Executive or HSE) was crippled by an attack that took months to fully recover from. Key events during the incident and recovery period include:

- Initial infection occurred on 13 h March 2021 with the threat actor spending 8 weeks in the environment before executing the ransomware.
- The threat actor executed Conti ransomware on 14 h May 2021 with the Health Service shutting down all systems.
- It took around 4 months to decrypt 100% of servers and restore around 99% of applications, which was not completed until 21s September 2021. In this case (and in contrast to WDHB) we understand that backups were compromised.

Business continuity plans did not envisage a severe but plausible total IT loss scenario. Much like WDHB, the HSE had no access to their critical systems, including those like the integrated patient management system for several weeks following the incident.

[8] https://www.group-ib.com/resources/threat-research/ransomware-2021.html

The findings from the *Independent Post Incident Review*[9] produced by PwC highlighted common themes with the WDHB experience. These included:

- Teams that included cybersecurity in their remit were under-resourced.
- Technology growing organically and becoming overly complex.
- The importance of effective security monitoring capability to detect, investigate and respond to security alerts.
- No documented cyber incident response plan that had been tested.

This is important context to consider when understanding what happened at WDHB. It was not unique in its position. The timing between the HSE and WDHB ransomware attacks was co-incident. It is important for Te Whatu Ora to use both these incidents as a catalyst to improve its own cyber security.

6 WDHB RISK ASSESSMENT AND CONTROLS

6.1 Capability and Level of Resource

Our Terms of Reference ask us to look at the WDHB level of preparedness before the breach occurred and the ransomware attack started. This assessment is both objective, and subjective. Objectively, we consider whether there were appropriate policies, controls and procedures in place ahead of the incident, linked to staff skills and training and incident response plans. Subjectively, we consider whether this level of preparation was reasonable considering the risks as they were known at the time both directly by the WDHB, and across the health sector. The resources available are relevant to this judgement.

Firstly, the objective assessment. The McGrath Nicol report on the incident completed for WDHB in February 2022 said WDHB had extensive policies and procedures in place that covered topics of cyber and information security, awareness, and response, and that the WDHB followed these policies and procedures in responding to the incident. They concluded that it is possible WDHB minimised the impact of the incident by taking action to prevent the deployment of ransomware across its systems. They said there were also no other containment measures by WDHB that could have contained the incident once they became aware of a compromise to its systems.

Yet, plainly the attack succeeded, at least in part. Separately, 9(2)(k) concluded in December 2021[10] that it was common for organisations to have an incident response plan. However, it is equally common for these organisations not to test the plan for functionality. WDHB was one of these organisations. It had an IT incident response plan with clear roles and responsibilities, but this had not been tested in a practice environment before the incident.

[9] https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf
[10] 9(2)(k), 9(2)(c)

This led to issues in the plan's practicality in some areas. For example, determining which systems should be prioritised for recovery and restoration.

9(2)(k), 9(2)(c)

[redacted] Staff to whom we have spoken clearly understood that cyber security needed to be taken seriously, and that in consequence there were expectations around their use of hospital systems. These plans were general responses and did not reflect specific threats or risks.

6.1.1 Recommendations: Risk assessments and procedures, capability, and resource

We note further on in the report that:

a) Cyber security skills are structurally short in New Zealand and indeed globally, and will need to be especially husbanded by Te Whatu Ora;

b) Planning for incidents needs to be realistic (i.e., pessimistic) and include realistic exercises, that allow response planners to experience and respond to significant adverse events. We recommend elsewhere that a virtual IT environment be established, so that health IT and data systems can be tested quite literally to destruction in a safe environment so that best responses may be evaluated.

However, on risk there is a further important recommendation. We look in detail at a subsequent WDHB analysis (from 22 June, discussed at length in Section 7, below) that highlights two sector risks: the very high degree of dependency on 'connectedness' – healthcare devices and systems only really work well for staff and patients if they get access to the data they need. Secondly, there are a lot of legacy systems in use that are important but have low security (they're often referred to as being in 'high trust' environments). High trust is good for people but not for IT as the trust level has, invariably, not been validated. As Te Whatu Ora integrates and consolidates, it will want to ensure it does not inadvertently create a larger and more attractive target, in particular by making assumptions with respect to trust.

That means standard cyber risk models might not be well calibrated for healthcare settings, although reports like that prepared by [redacted] in December 2021 nonetheless shed valuable light on the risks and steps that need to be taken. Specifically, we conclude that the WDHB's own analysis suggests data breaches might be more contagious in healthcare systems than others and have more severe consequences. Legacy systems frequently give rise to additional challenges when trying to maintain a secure environment as they may no longer be supported by the provider or manufacturer. Lack of systematic investment leads to legacy systems becoming entrenched and tolerated.

We take for example patching (which is an example that was not directly relevant to the May 2021 WDHB attack, but which is generally important). This is usually a routine activity in any organisation which considers cybersecurity important. However, legacy systems may not be patchable as they are perhaps no longer supported or there could be concerns around the stability of the system post-patch. This is further exacerbated by the

nature of the healthcare industry, where it can be life or death implications for an individual that these systems work, and work as intended. That's why the very conservative approach to security taken by WDHB and its partners immediately after the ransomware attack was right. Te Whatu Ora is putting a lot of effort into cyber security planning, which is welcome and necessary. Effective planning and security considerations from the start could greatly reduce the risk posed by legacy systems in the future. This needs to be well-targeted to allow for planning and resourcing decisions that reflect an accurate risk assessment. We therefore **recommend that Te Whatu Ora commission risk modelling based on actual health IT systems (Including legacy systems) to assess exactly how vulnerable they are to cyber intrusion and consequent compromise and degradation**.

This will help with the following:

a) Planning at a resource level, including staffing, skills and wider health workforce education, all of which we think will be constraints;

b) Calibrating control selection against the risks identified, i.e. performing risk assessments at various levels of abstraction to determine appropriate controls;

c) Identifying effective approaches to vulnerability management and access control,

d) Guiding technical architecture choices (see next section);

e) Planning exercises and thus building resilience - building on [redacted] comment at the end of their WDHB review in December 2021: Full Disaster Recovery (DR) exercises need to be practiced periodically, including, defined process and documentation for recovering applications where third parties are involved. In a major cyber incident, there needs to be a practiced plan to recovering services (not just systems) in a timely manner;

f) Training and supporting staff facing the consequences of successful intrusions, including managing the concerns of affected patients and staff, and supporting timely media and other communications; and

g) Providing a well-reasoned framework for compliance with legislation, especially the Privacy Act, by demonstrating "safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information".

6.1.2 Recommendations: Technical Architecture

IT system design can enhance or weaken resilience to cyber intrusion. Reports post-incident by 9(2)(k), 9(2)(c) have identified several issues that contributed to the WDHB's vulnerability and are the subject of recommendations for the future – most of which have, we were told, been implemented. We also note that since the WDHB incident Te Whatu Ora and the Ministry of Health have put a lot of effort and resource into cyber security planning. [redacted] also looked at cyber risk across the whole health system. Some of our conclusions and recommendations may therefore simply reinforce work already under way. They remain important.

9(2)(k), 9(2)(c) **it is important to design architectures that appropriately utilise gateway controls between environments, demilitarised zones (DMZ) to contain threats, and network access control (NAC) systems to prevent and detect threats, and to test their effectiveness before relying on them too much**.

9(2)(c), 9(2)(k) Overall, we still see the need for segmentation to be in place for all healthcare networks to reduce the impact of compromise.

9(2)(c), 9(2)(k)

Looking ahead, making future systems resilient to this and other vulnerabilities will be increasingly important as attacks and yet to be identified possible attacks continue. That will mean understanding and limiting vulnerabilities: the use of SOC/SIEM services will help (these provide continuous monitoring of security alerts, using both people and software); network segmentation and access control will be critical too. Combining these steps will not only reduce the probability of a successful attack but will also greatly diminish the potential impact any successful attack may have. 9(2)(c), 9(2)(k)
.
Looking ahead, we will also want to see systems resilient to failure, by design and through well-rehearsed response plans.

9(2)(c), 9(2)(k) 9(2)(k), 9(2)(c)

9(2)(c), 9(2)(k)

WDHB did carry out independent security assessments and monitoring of security controls on a regular basis. 9(2)(k), 9(2)(c) What emerges here is the importance of getting the narrative into focus – so managers avoid the "if everything is risk, nothing is a risk" outcome. A rolling focus on the most important five or so risks, and on treating them effectively, might be best. Ideally, risk assessment leads to the identification of controls required to reduce or manage the risk. Once implemented, these controls are then validated through testing, and then improved as necessary.

6.1.3 Recommendations: Operational Security

From an operational standpoint it's inevitable that software in healthcare will continue to evolve, both in relation to clinical care, and through connected medical devices. This innovation is welcome. The challenge is to keep it as safe as possible while securing the benefits. This is a governance challenge as much as a technical one. **Effective risk management frameworks, systematic rules on device connection, and a framework for retiring obsolete devices and software will all help.**

Technically, Te Whatu Ora should be looking at the use of DMZs and other forms of network segmentation to reduce the impact of compromise. **Effective segmentation is worth the possible inconvenience to reduce risks significantly, but each scenario will**

9(2)(k), 9(2)(c)

require its own assessment. The complexity of health data systems mean segmentation will always be complex and difficult to enable proactively. But the benefits are very real.

Security should be made as easy as possible for healthcare staff, including the technical staff needed to implement and maintain controls. As well as training and support on issues like access to systems, and clear rules on personal devices, **there should also be an information classification system from the outset** 9(2)(k), 9(2)(c) with associated protection guidelines (including encryption) and a clear framework for the storage and management of different kinds of data. i.e., having a good idea of where the most sensitive data is stored and how, of who can access this sensitive data and/or modify it. This is essentially a Role Based Access Control (RBAC) approach that assigns access to only that data which is needed to fulfil a particular role, and includes personnel and systems in its application. It will also be important to know what data is stored in the cloud and at what data centres, what data (if any) will be stored on premise; and in what scenarios should it be on premise. It's important that the decisions made regarding data handling are clear and well documented so that there is consistency for IT & Security staff as well as clinical colleagues in the organisation going forward.

Patch management is a challenge for the healthcare sector, with a huge array of services (often legacy) and diverse, complex IT environments. That said, WDHB commented that they were up to date on patching and that software vulnerabilities did not play a role in the incident (which is true). Nonetheless, **Te Whatu Ora should have a strong, empowered patch and vulnerability management program with the resources to stay on top of patching. They need to be supported by consistent, reliable asset management and assessment (so really valuable data is identified and properly protected), classification of data and physical (device) assets and determination of associated risks, a testing environment that allows for stability and efficacy of patches prior to deployment to production, and the appropriate knowledge to be able to deploy patches across the whole environment either automatically or manually in a timely manner**. 9(2)(k), 9(2)(c)

Finally, access and authentication systems. Te Whatu Ora has a real opportunity to pioneer a new culture as well as the adoption of **new technologies for authentication**, which could lead the way to getting healthcare staff used to and committed to multifactor authentication. This needs to be seen in the context of the clinical environment, so clinical staff are not expected to follow cumbersome or time-consuming procedures but will still benefit from effective multi-factor authentication, 9(2)(k), 9(2)(c) commented to us that Te Whatu Ora should start on the journey to a 'passwordless future'. This approach should be assessed amongst several options to find the best business fit.

6.2 Comment Investment

All of these are issues that, in an ideal world, would be tackled, or remedied. But the reality is that funding and resource constraints across the health sector will mean continued reliance on legacy systems and technology for some time. The result is a system that is, overall, weaker than we would want. The solution we recommend is a **systematic commitment to eliminate so-called technical debt (really borrowing from past investment) as quickly as possible. This will be expensive (as it will require investment to be accelerated) and will need to be combined meanwhile with compensating security controls** (tighter data segmentation, logging, and access controls for example). The result will be some loss of flexibility and utility for a time. But the alternative is permanent vulnerability. We judge that unacceptable and indefensible to the public.

6.3 Prior to the Attack

9(2)(k), 9(2)(c) : An important finding from the PwC Post-Incident Report of the HSE cyber-attack highlighted 'the cyber-attack was not actively identified or contained prior to the ransomware execution, despite the Irish Threat Actor performing noisy and 'unstealthy' actions." How was WDHB placed?

9(2)(c), 9(2)(k)

6.3.1 9(2)(k), 9(2)(c)

9(2)(c), 9(2)(k)

9(2)(c), 9(2)(k)

[redacted]

6.3.2 9(2)(k), 9(2)(c)

9(2)(c), 9(2)(k)

[redacted]

6.3.3 9(2)(k), 9(2)(c)

9(2)(c), 9(2)(k)

9(2)(k), 9(2)(c)

9(2)(k), 9(2)(c)

9(2)(c), 9(2)(k)

Operationally, the issue here is getting the balance right between a narrow, segmented span of control with high security, and a wider span which will be operationally efficient, but more costly – and risky - to manage. There is no 'right' answer, but it will be worth Te Whatu Ora considering this inevitable trade-off quite explicitly.

6.3.4 9(2)(k), 9(2)(c)

9(2)(c), 9(2)(k)

9(2)(c), 9(2)(k)

9(2)(c), 9(2)(k)

6.3.5 Overall

9(2)(c), 9(2)(k)

9(2)(c), 9(2)(k)

What does all this mean? Contextually, we note that a 9(2)(k), 9(2)(c) was a precipitating factor in the success of the ransomware attack on the Irish healthcare system at the same time as the WDHB attack. In the Irish case, some hospitals accurately detected the intrusion at an early stage and reported it, but nothing was done. This is material to our conclusions and recommendations. But it is a wider point – not related to WDHB – that IT hygiene (like patching) needs to be tackled in future with the same rigour as any other sort of hygiene in a healthcare setting.

Logging and monitoring must be taken seriously too: it is a crucial line of defence against all sorts of intrusions. Worldwide, organisations such as OWASP list a lack of logging and monitoring as a key risk and one that is often recognised during incidents. As the Te Whatu Ora data ecosystem becomes more integrated, the risks arising from cyber intrusions grow, and so defences need to be taken ever more seriously. For logging, secure systems must be built that can ingest information relevant for security teams, without also taking in sensitive information. These systems must also protect log integrity and forward logs to centralised services to allowed centralised monitoring. In turn for monitoring, 24/7 'eyes on glass' capability and the ability – and mandate - to act and respond in the moment 9(2)(c), 9(2)(k) . It is worth remembering that criminal gangs are active and imaginative innovators, with a strong focus on success. Any weakness will be found and exploited.

6.3.6 Lessons Learned

We recommend that **systematic logging and monitoring is mandated across the Te Whatu Ora data estate, including on legacy systems**. We know this is already planned, and indeed already in place in the former WDHB systems. What needs to be added to this plan is a commitment to action, so intrusions (and suspected intrusions) are actually and actively followed up and action taken. This is important and may be controversial, as it may include action that affects the delivery of healthcare services. We judge that this is a price worth paying, as the consequences of a large-scale cyber intrusion would be nationally significant. In comparison to this, the occasional false positive actioned by an empowered security team taking a proactive approach seems manageable and possibly even insignificant. **We also recommend regular exercising of incident response plans for healthcare systems responding to cyber incidents – something supported by literally everyone we have spoken to, and a central recommendation arising from the Irish incident**. We address this further, below.

We recommend the closest possible controls on the number and the activities permitted of privileged access accounts, including limiting where in the wider Te Whatu Ora network any one privileged account can operate. This will potentially be slightly inconvenient for those running systems, but a price well worth paying. And we also recommend **continued steps to segment networks, and to ensure that the configuration of systems, especially defensive elements like firewalls, are consistently maintained and actively assured**. We acknowledge that Te Whatu Ora will inherit a diverse estate of legacy systems, and so implementing these recommendations, as well as its own security

plans, will in practice vary over that estate. That diversity will be a challenge, but the objective should be for systems to be secured as much as possible.

6.4 The Incident: 9(2)(c), 9(2)(k)

9(2)(c), 9(2)(k)

-
-
-

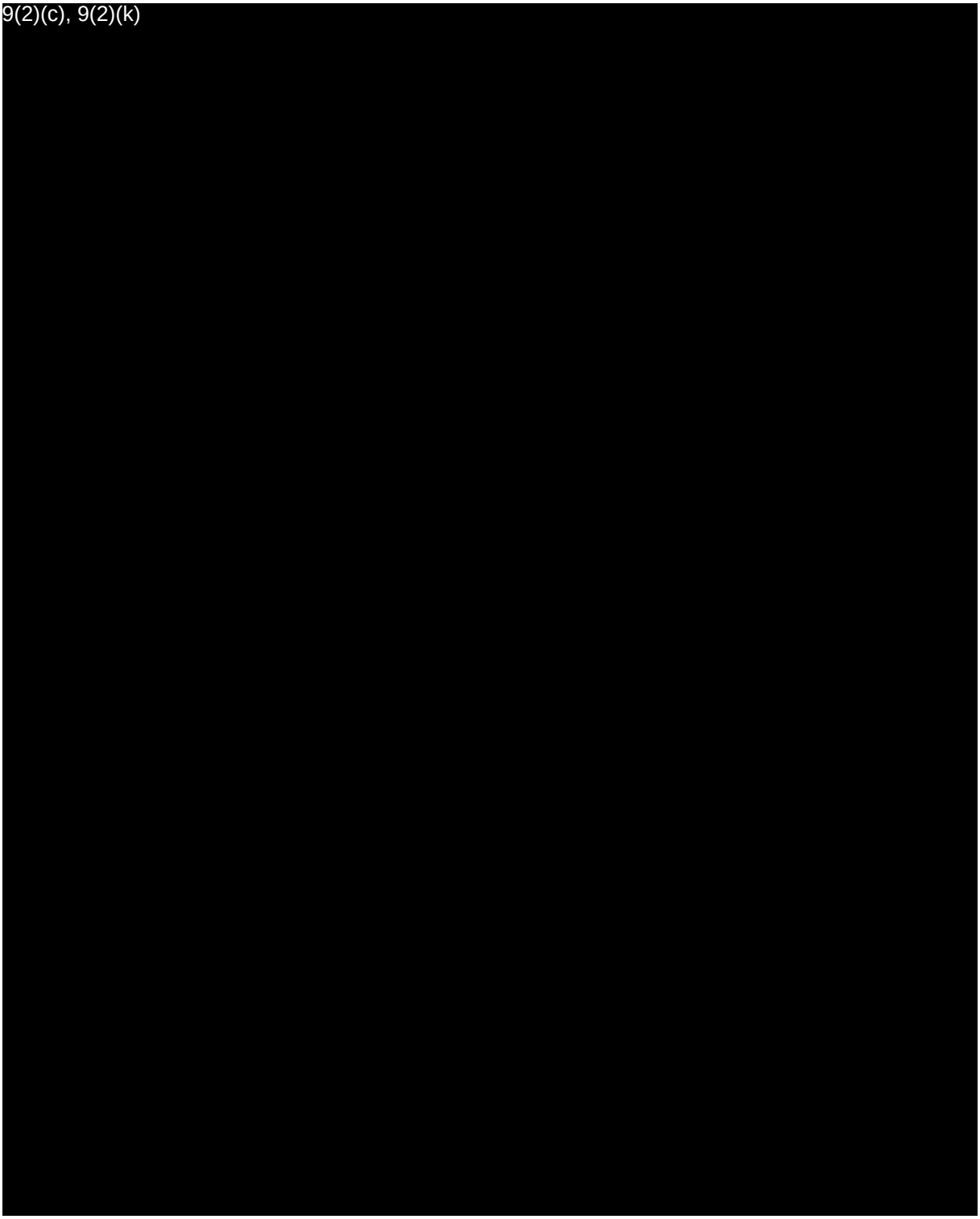
9(2)(k), 9(2)(c)

6.4.1 The Incident: Malicious Activity

9(2)(k), 9(2)(c)

9(2)(c), 9(2)(k)

9(2)(c), 9(2)(k)



7 DURING THE INCIDENT RESPONSE

When the incident occurred, the DHB's IT team clearly responded quickly and energetically.

Here we need to draw an important distinction between immediate response, and the system recovery process. The immediate response phase (as declared by the DHB) started on the morning of 18 May. On 26 May, the DHB moved to a Recovery (Planning)

mode. The DHB's timeline shows recovery mode on 31 May, while a move to Recovery mode is again reported on 18 June. We look first at the events of 18 May – the first day.

7.1 Immediate Response: 17/18 May 2021

The DHB immediately understood the seriousness of the IT incident even if the nature of it was not immediately understood. They also understood too that they would need to shut down the systems that had been or might have been infected with malware. Because of this step there was also an immediate loss of clinical IT services. The DHB also told the Ministry and the Minister's Office.

As a result, the DHB initiated its existing Coordinated Incident Management System (CIMS) arrangements. CIMS is a New Zealand wide all-of-government framework used by all government agencies for the integrated management of critical incidents. It is a widely recognised and well understood framework, which has been used in many contexts and is regularly updated. The DHB established an Incident Management Team (IMT) as a centrepiece of this system (this is quite standard within the CIMS framework). The question of an emergency response plan was later raised with us: the DHB explained that for IT incidents, its fundamental strategy was to recover the affected systems from backup. 9(2)(k), 9(2)(c)

As we understand it, the CIMS framework worked well on this occasion in managing the disruption to clinical and patient services. One issue we address later is that it did not and still does not include a specific arrangement for dealing with cyber or IT incidents (this reflects a significant CIMS whole-of-government concept and design issue). However, other than that important (but technical) point, we have not looked at the clinical response further as it is outside the scope of our report.

For the Waikato Hospital itself, the institution of an incident response from around 0800 on 18 May and the disconnection of systems led to the broader clinical system moving to manual, backup and other emergency management and incident management systems. These systems are beyond the scope of this report. The IT system focussed on isolation of its own systems and challenges. Overall, workarounds were put in place for most services, with some support from HealthShare (the regional shared service entity) and others. It's important to note that national Covid-related services, often delivered by cloud platforms, were not affected and continued to be available throughout this process, and indeed throughout the incident.

For the DHB's IT services, the immediate response, once the incident was identified as a ransomware-type attack, focused on isolating the DHB's systems from the internet, from Ministry of Health-supported systems, and from connections to HealthShare and other DHBs. The effect of this was protective of the DHB and wider Health sector's systems, but it also meant that clinical services were disconnected, even when they had not been directly affected by the attack. This was because the underlying IT systems provided the necessary connectivity for clinical systems.

A word of explanation: the Ministry provided WDHB with access to the Connected Health national IT service. The Ministry of Health told us that this Connected Health system was

disconnected from the WDHB once the Ministry learned of the incident. This is a nationwide system that brings all DHBs together. Connected Health is only one of a number of such services but is arguably the most critical because it connects DHBs to core MoH services such as the NHI service.

The disconnection was achieved by blocking the Waikato IP addresses on the system. The WDHB also disconnected itself. The WDHB noted that cloud services such as MS Teams and MS Office 365 systems continued to operate and be available. In addition, the Ministry told us it was greatly concerned about wider cyber risk to the sector at this point in the attack.

The Ministry told us that it saw its role at the start as keeping the Minister informed, watching and supporting the DHB's response, engaging with the Office of the Privacy Commissioner (OPC) and notifying the National Cyber Security Centre (NCSC). Later in the incident, communication between these entities became important. However, the initial response on the first day focused on system isolation and providing initial briefing to these other entities and the Minister. This was all done within the first hour or so after the incident notifications were sent, as everyone saw it as a significant incident.

HealthShare told us the same thing. They became aware of the incident themselves, due to interruption to the systems that they shared with the WDHB. HealthShare commented that, for them, the attack was a serious development because WDHB provided it (and all its participating DHBs) with operational services. They too moved to disconnect their other systems from WDHB systems, fearing contamination by what was at that stage obviously malware of unknown provenance and with potential for propagation through connected networks.

7.1.1 Comment: Disconnection

We have discussed the DHB's decision to move immediate disconnection (and the Ministry's and HealthShare's matching moves) with several informed interlocutors, both in Government and in the private sector. Universally, they think the DHB did the right thing (as did the other participants in networked services). We agree. 9(2)(k), 9(2)(c) [redacted] Given that risk, and the unknowns at the time, this was the correct decision.

There is a lesson for Te Whatu Ora in this too. When we look at the attack on the Irish national healthcare system at the same time, the reports disclose that some hospitals had detected the intrusion well ahead of the ransomware attack – during what is commonly called the reconnaissance phase. They reported this up the line, but no action was taken. In the WDHB's case, prompt action was taken. In various circumstances (we identify some more below) it will be important for Te Whatu Ora's IT and cyber security providers to have permission to act promptly, even when there may be an immediate adverse clinical impact. It is a theme we return to.

7.1.2 Comment: CIMS Recommendation

CIMS is a strong national framework for co-ordinated incident management. It does not currently have a cyber or IT dimension. We recommend that this be considered – CIMS analysis is predicated on a framework that looks at an incident through four complementary lenses: the social, built, natural and economic environments. None of these provides a natural home for cyber incident management, and we **recommend a fifth (networked or digital) environment lens should be considered**, and perhaps trialled. Furthermore, the CIMS framework provides for controllers to consider the resources available to them against an analysis of the incident they face, its impact and consequences. In the case of cyber or digital incidents, the resources available may include aspects of, or run over the same networks as the problem. The separation of problem and resource needs to be refined in these cases. These are technical considerations – albeit important ones – for central government.

The situation at the end of the first day saw the attack having reached its maximum extent – it was a single deployment of malware that did not go further. System and device isolation had been implemented, and back-ups were available. It's important to note again that WDHB's generic approach to disaster recovery for IT systems was recovery from backups, and that seemed immediately feasible. Provided steps were taken to ensure that the restored system was safe against further attack, the elements of recovery were, it seemed, already at hand.

7.2 System Recovery

Thus, for WDHB, having isolated the system, and identified the nature of the attack, the next step was system recovery. This was complex and took a good deal of time. Initial estimates provided to MOH proved optimistic. This was caused by both the growing focus on ensuring that the DHB's systems were not further infected, and because restoration processes are necessarily complex.

With hindsight, the service restoration process falls into several phases, as the DHB and the organisations and people helping to get things restored came to grips with the situation. It is important to note that the analysis we provide below is a hindsight one: like all history, this incident was lived forward and may best be understood backwards. That means the phases we identify, the judgements we have come to and the recommendations we have made are often ones not available at the time.

The IT service restoration process started immediately after the attack, but (as with the Irish incident) several IT services were unavailable for approximately two months. This time was longer than many of those involved told us they had expected. In reviewing the recovery, the timeliness of the process emerges for some as a central issue among those we have spoken to. Generally, Ministry interlocutors had expected the process to be faster than it was, and to show evidence of a clear plan. In practice, DHB interlocutors told us they had sought to manage expectations but the absence of a clear picture of the IT systems themselves, as well as the issue of ensuring that further malware was not either present or re-introduced made it impossible to provide accurate estimates. Others with experience of these incidents told us the time period was largely as they expected, but

that planning, and lack of a clear process was an initial issue for WDHB, at least for the first few weeks.

9(2)(k), 9(2)(c) [redacted] It took until 4 June to establish an effective service restoration plan and for services to commence being restored systematically. While this planning process was underway, some core services were nonetheless being restored. The DHB told us that the "Wave 1" IT core services had been restored by around 4 June and first 5 "critical" (or so deemed) "Wave 2" IT services went live on 11 June, that is 3 weeks and 3 days after the attack occurred. By 11 June the DHB had services going live and the next wave was planned and the WDHB had a plan to restore future waves. However, what the 'wave plan' didn't provide was a timeline because the DHB didn't know how long it was going to take to get each service restored.

That said, the basic approach was clear and sensible from the outset: to recover by using backups. This was the WDHB IT disaster recovery strategy, and the cyber-attack was a type of IT disaster recovery event. The approach worked, although a more granular, and practiced plan addressing cyber-attacks would have been better. It took longer than many expected (as discussed above) and revealed complexities around the way IT systems were used in healthcare delivery. The first issue related to the security of the restored systems.

7.2.1 Phase One of the Recovery: 19th – 27th May

We have set the period for the initial recovery phase as being from 19 h – 27 h May. May 19 h was day two of the attack and when a plan beyond disconnection was starting to come into focus; 27 h May marks the day that a more prolonged and apparently more carefully managed recovery process would be commissioned. At this point, 9(2)(k) were also engaged to review the recovery process from that time. Over this first period, three broad areas of effort took place:

- **forensics** work (to work out who the attacker was, and how they got in);
- **recovery** work (to get systems back up); and
- **security** work (to make sure the restored IT systems were safe from further or residual attack).

Over this period, a substantial number of servers were able to be recovered from backup, into quarantine. This meant they were brought back within the data centre, and onto internal networks, but not connected to the wider internet or to external partner systems.

However, this did not translate into restored clinical or other services. This reflected the underlying complexity of the DHB's IT systems, and the number of clinical and support systems that needed to be restored. Essentially, servers did not map directly onto systems. It also reflected the conundrum that quickly emerged: the handling of residual risk to the systems meant it was very hard to know when it was safe to reconnect. This became a central issue for the month ahead.

From the outset, the DHB's IT team and a number of external providers were hard at work:

- 9(2)(k), 9(2)(c) were working on the attack itself, analysing logs where possible. This was the forensic work, with a national security element;
- 9(2)(k), 9(2)(c) was taking steps to make safe the IT systems for restoration following 9(2)(k), 9(2)(c) designated process 9(2)(k), 9(2)(c) systems were those mainly affected; and
- 9(2)(k), 9(2)(c) was preparing to undertake further forensic work later in the process in preparation for restoration. This process would not be able to fully begin until the servers and end points were alive and connected again.
- 9(2)(c), 9(2) was engaged to provide external cyber security assurance, with a focus on the threat actor, and on trying to ensure rigour in security processes.

These processes were underway within the first two-three days.

Right at the start 9(2)(k), 9(2)(c) correctly identified the ransomware malware as the 9(2)(k), 9(2)(c) product, as described above. We have seen 9(2)(k), 9(2)(c) . This accurate technical attribution meant it might have been possible to assess whether the attack was likely to proceed further, based on the known technical features of 9(2)(k), 9(2)(c) and the way it was typically deployed by criminal groups. Essentially, 9(2)(k), 9(2)(c) was a prosaic criminal tool, with limited risk of persistence, and perhaps unlikely to be associated with other types of attack.

In considering this, two lines of explanation have emerged. One is to see this insight as a possible opportunity to speed recovery – which leads to the question why did it possibly get missed? Would it in any case have been too much of a risk? With hindsight, DHB interlocutors described a sort of 'imagine the worst' mindset emerging, with fears of a more persistent, capable, and aggressive adversary leading to excessive caution. This mindset, we were told, formed as part of the feedback that WDHB was receiving from its trusted external advisors 9(2)(c), 9(2)(k)

But there is an alternative view: that caution was prudent: that the attack wasn't just an outage, and it wasn't sufficiently well understood to support any conclusion other than one of real caution. It was certainly more than a simple outage and needed real care to ensure that additional risks to both WDHB and the wider health system were contained. Based solely on attribution of the malware variant to 9(2)(c), 9(2)(k) and given the limited technical information available at the beginning of the response we judge there couldn't have been a high degree of confidence at the start that the attack was over. As noted above, this malware is offered as a 'Commodity Ransomware as a Service product', meaning any number of actors with a wide range of intents could have been responsible for the incident.

Given the actor also demonstrated an ongoing interest in exerting additional pressure on the DHB, e.g. through ongoing engagement with media, we were told it was reasonable to assume that they could have retained additional access to the network and so repeat

victimisation of the DHB's networks was a real risk to be considered and balanced alongside service restoration.

The DHB needed to make an informed risk-based decision on how quickly to restore services. They were in a tough place balancing growing clinical need with security and significant unknowns. As we shall see, the balance of this judgement evolved over the following month.

And as noted above, what was lacking **was a systematic assessment of the situation, drawing on forensic and behavioural insights, to reach a shared appreciation of both risks, and recovery opportunities. We recommend that such a systematic approach be adopted by Te Whatu Ora as part of its cyber incident planning and practicing.**

That gap mattered. We judge that it created a level uncertainty, which combined with the sheer volume of effort involved, and the consequent need to ensure that new cyber threats were excluded from the recovered system to mean that for this part of the recovery phase immediately after the incident the WDHB did not and perhaps could not have developed an estimated timeframe for full return of IT services, especially because the nature of the assurance task kept growing.

As this first week progressed, the question of testing and approving reconnection to the wider Health system and the internet loomed larger. Servers and other systems were being recovered, and internal connections tested. But wider reconnection raised the question of repeated infection and led to the question what level and sort of security arrangements would be needed in the recovery process.

As we show later, by 22 June, the DHB had explicitly decided to move ahead with service restoration, consciously balancing the pressing need to get the hospital back into full operation against residual security concerns. This decision reflected a combination of overriding clinical need, and – by then – a month without further incident, and some significantly tighter cyber security arrangements. We certainly think that was the right decision at the time. The question is whether the insight to the nature of the ransomware could have been a basis for an assessment that might have supported a quicker move to full restoration without the tight security requirements initially in place. The conclusion we come to is that information like this was potentially valuable but would need to have been subject to a proper assessment process.

9(2)(c), 9(2)(k) [redacted]

Beyond that it became clear that a significant, complex restoration process would be needed. Looking ahead, by early June this had led to the development of a comprehensive plan based on a series of restoration 'waves', bringing systems back into service broadly in order of priority. This was itself a complex planning process, which concluded around 4 h June, the same point as the restoration of the first 5 core services occurred. Much of the success of the 'wave' process was, we were told, the result of an informal process that brought clinical and IT people together to ensure a good

understanding by both of what was required clinically and how the IT systems actually worked. **We conclude that it will be important for Te Whatu Ora to ensure that clinical and IT teams plan for both security and incident response in close and permanent co-ordination.**

By now (even after the first few days) it was also being concluded that a more systematic approach to the security of the restored system was needed. The first response was to add an explicit risk management framework to the recovery process, commissioned on 24 h May. This was an internal process, looking at:

- Existing strategic risk, including plans in place to mitigate and resolve those risks
- Risks that contributed to the attack
- Risk created by the attack
- Change control risks
- Risks of recovery, rebuild and transition to an operational state
- Confirmation that the system was clean as a result of the recovery, as well as operational risks before, during and after the attack
- New ways of working, and associated risk/benefits
- The impact of the change in security posture based on the attack experience

This was comprehensive. However, It was also managed by the same team managing the recovery, adding to their already immense workload. That also meant the risk management framework reinforced the assumptions of the team on the ground and their advisers, rather than challenging them.

The same day, concerns about the need to improve change control disciplines though the recovery process were being articulated, putting the team under further pressure. The broad approach was to minimise connections to the wider health system ('pinholes' in what later became known as the 'hard shell' of disconnection). This limited connectivity, testability and really reduced underlying clinical usefulness. But it did provide a basis for restoration work that allowed progress to be made, albeit in a decision-making environment focused rather too narrowly on further cyber risk.

At the same time, pressures were building elsewhere: The DHB was operating on manual systems. The Covid-19 response was well under way. While these systems clearly worked, and patient safety was largely assured, the additional effort was starting to tire staff and thus affect patients. Staff were being reassured about salary payments, but we understand that nonetheless for some, questions remained. Shift and roster patterns would come to be affected, and staff would want to be able to book and take leave. Prolonged manual running was, it seems, feasible but undesirable, and just hard work for already hard-pressed people.

The attacker's disclosure of potentially sensitive patient data (and the associated concern that more data might well have been exfiltrated) was also of concern. Communications between the Ministry and the DHB had become difficult. The Ministry saw the DHB as not

communicating as the Ministry expected; yet the DHB set out quite a different view; it saw itself as providing constant, accurate formal and informal communication, with daily SITREPs and calls, involving the CEO, as well as management and IT teams. The DHB saw itself as grappling with increasing 'unknown unknowns' as fears of continuing cyber incidents were unabated, and as an undoubtedly stressful and demanding healthcare delivery situation was managed. At a governance level, there had emerged a genuine question of roles between the two: in 'normal' times, management of IT incidents would lie unequivocally with the DHB. But in this case, a serious incident with potentially national consequences, the Ministry's traditional oversight role necessary faced pressure to step in. In practice, the decision taken around 27 h May resolved this in favour of active involvement.

The Ministry became concerned too. Initially, they had seen the incident as one for the DHB to manage, taking account of the need to ensure the disconnection of the DHB from wider health data systems (quickly accomplished). But as the first week after the attack wore on, the Ministry saw the DHB as needing more help, and became concerned about the restoration process, as well as managing media and related privacy issues.

GCSB's involvement through NCSC (the latter is an operating name of the former) included understanding how the attack happened. We have seen the relevant redacted summary of this work, and this is reflected in our report. Our focus has been on ensuring that risks of future attacks like this (and others) are understood and minimised, and that the health system (writ large, including both Te Whatu Ora, and the legacy systems and structures it will inherit) is well placed to respond when cyber-attacks do occur (as they inevitably will, over time). Our recommendations and underlying judgements also reflect some NCSC input, for which we are grateful.

7.3 Media & Communications

One issue that emerged as a critical piece of the DHB/Ministry relationship was briefing and support to respond to media inquiries. The attack was a subject of intense media interest, intensified by the disclosure of some patient information by the attackers. The Ministry has primary responsibility for supporting the Minister but relied on information provided by the DHB. This arrangement became somewhat strained. This was because while the DHB was accurately reporting what its team had done, the DHB's own grasp of what needed to be done was evolving, and so early estimates of the time it would take to restore services proved optimistic, complicated by different expectations as to what 'restored' meant from an IT as opposed to an integrated system perspective. Both MOH and WDHB paint a picture of a frustrating set of interactions, each considering themselves unheard by the other. The DHB's IT team met the Minister on 17 June, which may have helped establish some confidence.

This had the potential to become a source of real distraction for those involved. Given the near certainty that cyber security incidents and data breaches will occur again, it is worth considering how to balance the need for the IT teams to focus on the operational issues, while keeping ministers, senior officials and regulators, as well as patients and the wider community informed of and able to intervene if needed. We **recommend that effective media briefing and communications form an integral part of Te Whatu Ora's cyber**

response planning and practicing. We also recommend that media professionals be fully integrated into IT teams dealing with incidents, and able to engage with Ministerial and government media and communications teams seamlessly and with a high degree of autonomy. Finally, and this will be a challenge for Te Whatu Ora, there needs to be an explicit effort made to **avoid the trap of false hope or unfounded optimism in briefings**. However well intentioned, our experience is that response, recovery and restoration processes almost invariably take longer than initially foreseen and lead to more complications. This truth needs to be embraced.

7.4 Privacy Issues

On 25 h May the Ministry became aware that data stolen from the DHB had been passed to the media. This was unwelcome news, but not entirely unexpected as this was and remains common practice for ransomware operators. This added a privacy dimension to the incident.

This raises the question of the management of public expectations in future where what might be termed 'mass disclosure' of health information takes place. This is a likely future contingency, as cyber-attacks will continue, and we must expect even a small proportion to succeed. Attackers have little interest in anything other than monetising what they can, and we know that health data has real value on the illegal market. So, what do we do?

The relevant regulator is the Office of the Privacy Commissioner (OPC), an independent Crown Entity. Without in any way fettering either the Commissioner's discretion, or the full scope of the Parliament's oversight, we considered whether there is merit in Te Whatu Ora seeking to engage with the Commissioner, to develop an indicative Code that would guide Te Whatu Ora's response to significant disclosure events and give the community some sense of what they might expect in such circumstances. On balance, having consulted OPC, we have concluded that such a step would not be necessary, as the Privacy Act 2020 gives OPC sufficient scope to both respond and to support Te Whatu Ora as required.

OPC explained that the notification obligations in the Privacy Act include notifying affected individuals as soon as practicable after becoming aware that privacy breach has occurred (section 115). Where it is not reasonably practicable to notify individuals, public notice must be given (section 115(2)). In the context of the privacy breach at WDHB, that included public notices about the disruption to services resulting from the attack (the action that prevented the DHB from access its information on either a temporary or permanent basis was, in itself, a notifiable privacy breach – see section 112), as well as ***initial*** notices relating to the exfiltration of information once that had been identified by the DHB. Section 115(4) makes it clear that organisations must notify individuals at a later time if the circumstances change so that public notice or an exception in section 116 no longer apply and there is or remains a risk that the privacy breach will cause serious harm to the affected individual or individuals.

7.5 Governance & Risk Management

This first week or so of the restoration process is a story of risk. Despite the accurate technical attribution of the attack to 9(2)(c), 9(2)(k) software, the recovery process was increasing focused on the unknown (but we now know, very low) risk that the attacker was still lurking in the WDHB's systems. In future, incident controllers should be provided with behavioural advice to help calibrate apparent risks against likely attacker conduct. Cyber-criminal profiling needs to become a thing for Te Whatu Ora. Ransomware type attacks are now so widespread globally that statistically meaningful data sets related to the outcome of attacks, and the conduct of attackers should be able to be assembled and used to derive behavioural insights with some confidence.

Otherwise, this set of events will be repeated, and perhaps less well-managed: in the absence of countervailing advice, decision makers faced with unquantified risk but with enormously serious consequences will almost always see the right decision as being to seek more information or assurance. For WDHB in late May 2021, the situation was literally unprecedented, and there were many voices telling decision makers that unacceptable or just unknown risks remained. The result was elaboration of controls, initially without a clear road to restoration. Looking ahead, it was as the clinical costs became evident that the DHB, courageously, grasped this issue and made the right call.

What should be done? This will be a big issue for Te Whatu Ora. We recommend that executive level managers exercise these scenarios and **have access to well-researched behavioural advice around the conduct of cyber criminals**. We understand that this is already planned. The relevant attacks are always going to be criminal. Behavioural insights will be available and should be used. While we have focused on the health sector, these recommendations are ones that might well apply across government.

7.6 Phase Two of the Recovery: The 27th of May Changes

So, by the end of the first week, these issues were mounting. It was clear that a bigger restoration task lay ahead, and that the question of providing security against further (or continued) attack for the restored systems (and those it connected to) was unresolved. Over the following month, solutions emerged.

That process can be seen to have started on 27 h May, when the then CEO of WDHB, Kevin Snee, met the IT team's management. He set out the continuing impact of the attack and restoration process on the hospitals and on patient services to the team's management. He noted frustration with the pace of service restoration across wards, staff and patients. Ministry of Health officials were also in the DHB the next day, also reviewing progress. As a result:

a) A plan was commissioned to specify firm dates and times for the release of applications;

b) 9(2)(c), 9(2 were brought in immediately to review and assess the risk of systems and applications being brough back online (looking ahead, they reported on 11 June but elements of what later appeared in their recommendations were evident from when they were engaged on 28 May); and

c) It was agreed that sign-off for systems and application to be brought back online would lie jointly with the CEO and the Ministry. [redacted] input was intended to underpin this process.

In the regional and national health system (involving HealthShare, its member DHBs, and other regional DHBs), there continued to be support provided for WDHB. This included remote working hardware and access, e-pharmacy, and other systems.

7.6.1 Phase Two of the Recovery: Comment & Recommendations

We think this intervention was right but could have been better: the DHB's team needed support, including from the centre (the Ministry at the time; Te Whatu Ora now). Issues around the security of the reconnected system needed careful consistent management to tackle national consequences.

Furthermore, the communication of progress, resolution of issues, and consistent management of privacy and other questions all required proper coordination, which started to improve from this point. From this, we can draw the conclusion that the networked nature of current and future health data systems means a significant breach anywhere in that complex ecosystem exposes potential vulnerabilities everywhere. However, those vulnerabilities need to be really understood, and the inevitable incidents assessed and not catastrophised. That leads to the conclusion that Te Whatu Ora needs to be able to respond to future cyber incidents seamlessly, drawing on national resources from the outset, on the basis of thorough preparation. It leads too to the conclusions and recommendations that:

a) **Planning for future health system cyber incidents needs to be undertaken at a national level, and subject to testing, training and practices at a national level**. This is similar to recommendations arising from the Irish incident. It is important to note that planning for incidents involves the whole system (clinical, IT and managerial elements) and assumes the worst. It is different from, although complementary to the work already going on to *design* strong security into the Te Whatu Ora IT system as it evolves. This latter work will reduce risk and increase resilience; the incident planning we recommend will prepare for times when cyber breaches are successful; and

b) Cyber security skills are structurally short in the New Zealand economy. **Building and maintaining a national skills capability (perhaps as a centre of excellence) for health-related security expertise should be a priority.** Effective incident planning requires effective incident management capability to be on hand. There is good research (dating back to the Haldane "*Report on the Machinery of Government*" of 1919!) that when public sector skills are short, they should be concentrated, so that their deployment is optimised, and their quality maintained. The resulting skills and expertise could always be shared with other jurisdictions (e.g., Australian States). But we consider it essential that Te Whatu Ora has its own capacity to respond. Anything less puts the benefits of a digitally enabled health system at risk. We note that there

may be thoughts around regionalised security arrangement for Te Whatu Ora. We see this is sub-optimal and may be actually risky.

7.6.2 Other Developments in the May 18th-28th Period

The attacker sent an extortion email to the DHB on 23rd May. There was never any question of the demands being met. This is MOH policy and is the correct response.

It's important to note that the clinical impact on patients – although real, especially at the start -was a lot less than might have been, because of the effectiveness of the CIMS process, and the extra effort made by staff through the DHB and its partners. There were very few patients referred to other DHBs because of the actions taken across the DHB. Although the incident was not formally closed out till the 10 h November 2021, most services were back much sooner.

A central issue through the recovery phase was the lack of understanding of the integration and dependencies of healthcare IT services across the DHB. The DHB's restructuring in recent years may have contributed to a loss of tacit knowledge, but this possible factor lies beyond the scope of our inquiry, and we have not pursued it. Two other important points were at play here:

a) Lack of experience tackling large scale cyber-IT incidents, including in the otherwise well-understood CIMS framework. This included the need to practice a restoration; and

b) A lack of understanding of how the healthcare IT data ecosystem worked, so that planners initially struggled to see the link between services (what the patient or clinician saw and experienced) and systems (what the IT folk were fixing). The recovery period saw both these issues tackled, ultimately effectively. But both took time, as the underlying complexities and knowledge gaps spanned the whole New Zealand healthcare sector, not just one DHB.

Interviewees consistently described to us a process whereby the CIMS process and the IT recovery process initially operated in parallel, with the IT process initially focused on server restoration rather than service restoration. Restoration was possible at each point using rebuilt machines and back-up data, as well as re-entered data where necessary.

But the focus on servers was of limited utility as it was not clear to the IT team (housed separately from clinical teams and reportedly quite divorced from a lot of clinical practice) how servers connected to services. The team did have a mapping of applications to servers, but what they didn't have a good understanding of was the mapping of applications to services and the dependencies between applications, and what other external systems and web resources and systems would be needed to bring about actual service restoration in the clinical or patient environment. This meant even when the incident response team remediated a significant number of servers, this did not necessarily translate into the effective restoration of services from the viewpoint of the hospitals.

All this took several weeks to play out.

After the CEO's intervention and the engagement of [redacted] around 28 h May, two related processes emerged:

[redacted] looked hard at the security requirements for safe service restoration (really reconnection to outside systems by whatever means, from the web to dedicated VPN connections). This led to a sober but – what seemed at that stage - realistic set of rules, submitted to the DHB [redacted] on 11 h June, for an 'Authorisation to Operate' (really permission to reconnect) protocol or set of rules for the re-activation or re-connection of systems to the wider health and internet-enabled data ecosystem. [redacted] provided a comprehensive analytical framework for this process. It was reinforced that final sign-off lay with the CEO and the Ministry – something agreed around the time [redacted] was first engaged. This cemented the Ministry's new role as an active participant in the restoration process;

b) The so-called 'wave plan' for restoration was developed quite quickly (as described above), in the week ending 4 h June 2021. This described restoration through a series of complementary 'waves' of activity, intended to restore services in clinical priority order. In fact, it was a real breakthrough, because it addressed the whole complex system of systems, showing the full task ahead. And, crucially, it reflected clinical input. Because it reflected clinical input, it was something the planners could focus on, and work with confidence. This met the requirement for a clear plan. We were told that it was the result of a fruitful engagement between the IT team and a small clinical group. That co-working across disciplines is of course a classic diversity-of-thought model, worth building into future incident response plans;

The DHB itself then produced a compelling analysis of its IT restoration predicament on 22nd June. This analysis – one of the most important single documents of the whole incident – entitled "*Re-connecting to the Digital Health Ecosystem"* was in many ways a turning point for the DHB's – and the Ministry's -understanding of the issues they faced. It confronted the risks, paved the way for the smooth restoration of services over the remaining period of the incident, and really marked the point where the DHB and its support team got on top of the ransomware problem, because they had really come to understand the way the underlying systems operated. It's worth a further look for the insights it offers.

7.6.3 The 'Re-connecting the Digital Health Ecosystem' Analysis

We've given this paper a lot of attention because it was the moment when the tension between clinical need, and cyber security of the restoration process was addressed squarely. It should be required reading for anyone looking the prepare for or manage health IT and privacy incidents.

The key insight that this analysis contributed was that full connectivity was essential for clinical services. It said that a modern healthcare data system needed real time access to a wide range of data and in some cases diagnostic sources, many of which lay beyond the IT perimeter of the hospital, or the DHB, or even New Zealand. Restoration of services required reconnection – even rapid reconnection - to the wider world. Partial or attenuated connection didn't work – WDHB had tried that.

The analysis went on to highlight the conundrum: the level of detailed analysis required to reconnect services with absolute security would take too long, given the toll that manual working was taking on staff, patients, and the wider health system.

This reflected the experience of the period from 28 May to mid-June, working with the so-called "Hard Shell", set up to protect the DHB, its patients and staff and the wider health system by maintaining minimal connectivity with other entities via the internet or proprietary networks such as Connected Health. This was proposed and agreed on the assumption that this state would be maintained for approximately a month, over which time, improvements would be made to further strengthen the DHB's security.

The DHB's own analysis said that the experience of working within the hard-shell framework had shown that:

> "the level of digital co-dependence with external health providers and the dependence on the Waikato DHB by other DHB's (for example Lakes) has been bought to the surface – highlighting a significant issue for the DHB to address; the ability to sustain the "Hard Shell" given the now apparent and increasing clinical risks associated without having the previous connectivity. After nine days of use of Wave 2 applications in a degraded state, networked services that were considered peripheral at launch are now considered critical given manual processes and overall organisational fatigue."

In other words, for the sake of patients and staff, things had to change. There were now over a hundred web sites that were considered essential for clinical services. As work progressed, more and more web sites were surfaced. This was a process of discovery for the IT team, to learn just what was needed to run services. We think it was equally valuable for the clinical contributors, who also saw how much their work was dependent on effective networks.

7.6.4 Revised Risk Position

As part of the ATO process, the DHB explained that it had adopted several significant controls to manage and reduce cyber and business continuity risk.

The technical controls included:

- 9(2)(c), 9(2)(k) [redacted]

- 9(2)(c), 9(2)(k)

As a result (or coincidentally), the report then noted that there had been" zero evidence of residual malware detected, nor of the Cyber Actor being resident in the network". Notably and importantly, there had been no evidence found of a breach into the medical networks from the corporate networks. The DHB said that "the Cyber Actor appears to only have gained access to the corporate network, not the beyond into the medical network". It noted that forensic investigations as continuing, and that this might change (in fact it didn't – the attacker had reached their maximum extent on the first day).

The report went on to note that the controls had highlighted the many points of interconnection with the rest of the health sector and the deep clinical integration. It also identified the nature of the inter-connectivity, particularly associated with the medical domain, which operates in a highly trusted mode (i.e., low security) across the sector. The report went on to note that "The challenge that is being worked through is many of the digital services were implemented and designed to operate in closed and highly trusted networks. Most of these solutions were implemented many years ago and carry with them the residual risks associated."

This is the legacy challenge that Te Whatu Ora now faces too: This sort of high trust/low security inheritance will be a significant feature of the New Zealand health data ecosystem for some time. They are vulnerable to attack.

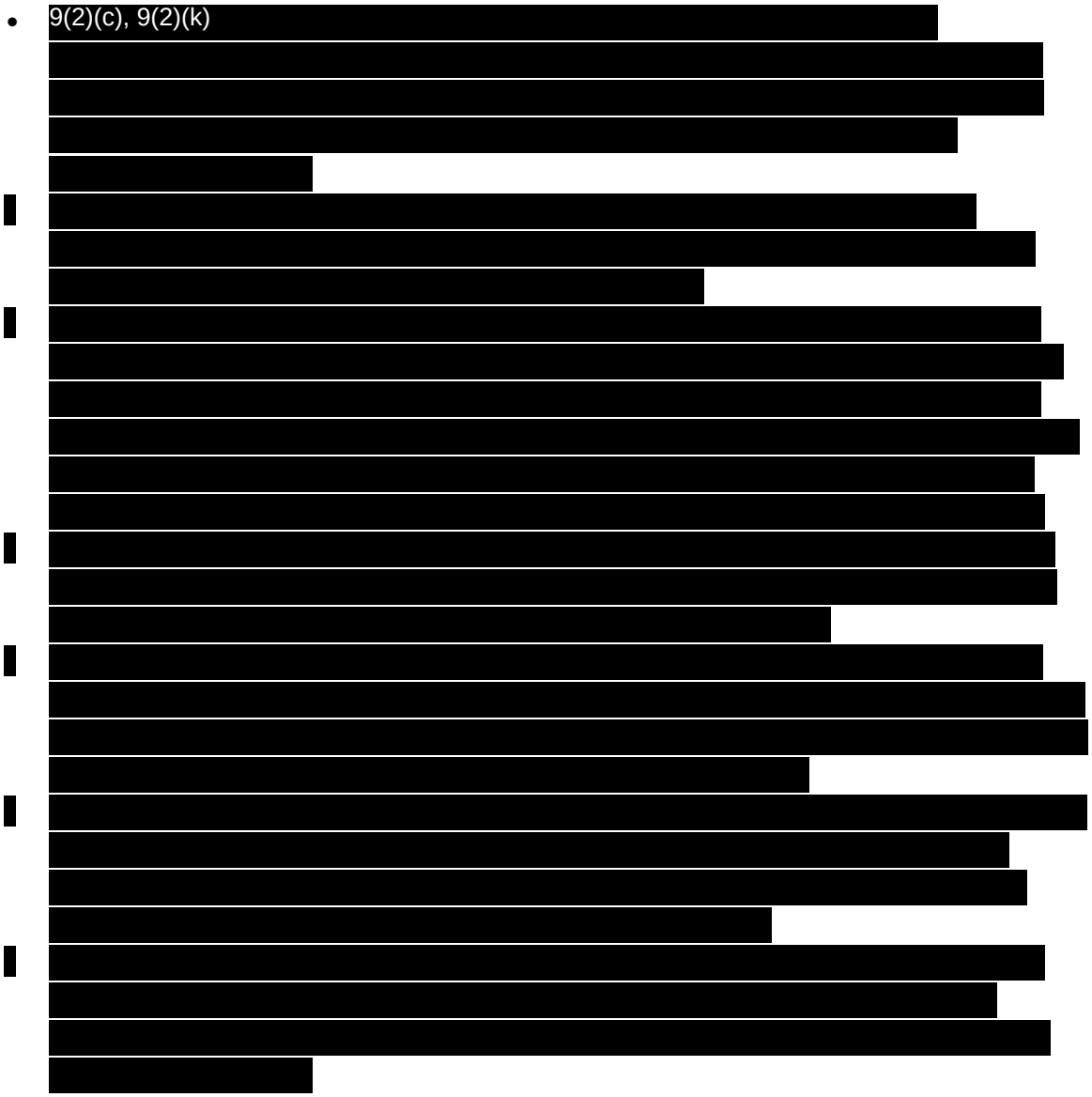
The DHB team went on to recommend accelerated reconnection, balancing the best security controls they could put in place against ending the clinical and patient service degradation they saw starting. The result was a proposal to achieve "a balance of cyber risk against patient and employee safety … associated with the prolonged outage and

disconnection of application services." They went on "it is not considered feasible to assess each and every service upfront, nor likely that changes to mitigate risk be able to be achieved in a reasonable time period".

The result was a proposal to "address our connectivity needs (all subject to technical change control). This action will unblock all services within Wave 3, 4 and beyond as well as Wave 2 services that are now considered non-viable due to connectivity and the associated manual workarounds". In other words, it would get the DHB and associated services back in business. Clinical delivery had won; tight security came second from that point as the balance of risk had shifted from security to patient and staff services.

Detailed re-connection and security steps were proposed, but essentially, they re-lit the networks much as they had been. These included (we've quoted verbatim):

- "Restore health network services collectively to the last known configuration, including – target Thursday:
  - 9(2)(c), 9(2)(k)



- In parallel (i.e., not holding up the process), review each service to fully assess its risk, propose and consider effective treatments for those risks and implement in a considered manner – to be completed over the coming 6 weeks."

This decision paved the way for an orderly restoration of the remaining services over the following months. It meant that aspects of security were certainly stronger, but there was also a strong back-to-how-it-was element. As noted above, the 'wave' plan came into its own, and provided the framework for this complex process, with a good focus on clinical need. The wave plan itself provides something of a guide for future restoration tasks, at least in concept. We have not repeated the detail of that process here – it was of little security interest.

8 POST INCIDENT

8.1 Findings

What did all this mean? As the foregoing shows, after the first day, there was a kind of pendulum effect:

a) An initial focus on tight security, against the risk that the intruder was still in the system (one interlocutor called this the 'active shooter' phase). This led to a risk process being loaded onto the team (without that becoming a useful challenge function), then to the 'hard shell', and the ATO process. Security was tight, reflecting conservative, risk-averse views at the outset;

b) A growing realisation that the clinical and operational needs could only be met by full connection. The development of the 'wave' plan through a synthesis of clinical and technical insights was at first sight extraordinary, as the IT team initially lacked a good insight into the way healthcare was delivered, and vice versa. Rather, we see this discontinuity as the result of a genuine cultural gap which we think likely to be widespread: as the health data ecosystem had grown and grown quickly in recent years it had in some important way grown onto the underlying IT system, not with it. The result was an underlying gap in understanding (which we emphasise was on both sides of the process – service and system) that compounded the other issues we have identified; and then

c) The Hegelian synthesis (how we've longed to use that term in a cyber security report) of the risk and recovery pressures through the 22nd June document, and the way ahead it established, balancing rapid reconnection with enhanced security, where possible.

8.2 After the Restoration Process

The DHB became confident of its ability to recover from backup, as part of its wider disaster recovery strategy. However, the remaining, ongoing issues (largely set out in the subsequent [redacted] report) include a lack of process and documentation for recovering applications where third parties are involved.

That said, the recovery process has led to a lot of improvements since the attack (along the lines of our likely recommendations). 9(2)(k), 9(2)(c) [redacted] These are material improvements that reduce both the likelihood of another successful attack and the impact it may have.

8.3 Wider Lessons for the Sector

At first sight, the necessary recommendations for the wider sector seem simple, even obvious. But each comes with significant underlying cultural changes:

- Permission to act: Logging and monitoring are only useful if it is accompanied by permission – or a requirement - to act on indications of compromise, even if this means interrupting or affecting services. IT security thus must move from a background role, to one that potentially intrudes on delivery (hopefully briefly). That's a big ask. But the risks to the whole system (magnified as a national data system emerges) mean that the management of the healthcare system needs to be consciously undertaken in an environment of continuous low-level conflict.
- Mandating that the Healthcare system undertakes planning for such incidents seems obvious. But that will mean a revision of the CIMS model (a whole of government undertaking – worth doing but not trivial). It will also mean requiring healthcare delivery colleagues to co-operate, by following rules in connecting systems, using new devices, and accessing data. Without that co-operation, any plan will be dangerously unconnected from the reality of the systems it seeks to protect. This will be a big cultural shift for many, including hard-pressed clinicians. There is no real alternative, but it should not be underestimated. It should also mean ensuring data is structured in a forensic-ready way, so incident response and investigation is facilitated.
- When incidents do occur, the response and transition to recovery needs to be 'intelligence-led". That's not a mandate for the NCSC; it's a way of describing the way the incident managers need to be able to use technical and behavioural information to draw defensible, testable assessments and inferences about the likely behaviour of the attackers. The identification of the 9(2)(c), 9(2)(k) malware in this case was a possible catalyst for such an analysis. It might not have changed immediate steps, but the 22 June shift might well have come sooner. Te Whatu Ora needs to have the skills. Information and practice to get it right next time.

Implicit in all of this is our view that cyber security is a continuous process in an environment of permanent challenge. It will never be 'solved'; rather; the criminal threat to our data must be managed down, designed out, and then ultimately accepted at a genuinely residual level. This is a task that will never be finished. That means changes in

attitude and behaviour across the whole system, by everyone. It means more resources – money and skilled people – if it is to be effective. Above all, it can't just be left to the IT folk.

8.4 Recommendations

As discussed above, the design of a digitally enabled healthcare ecosystem requires IT services to be put on balanced footing with clinical services. As shown through the impact to delivery on health care services throughout the restoration following the cyber incident, the system cannot function effectively without the core IT services operating. Looking ahead to the changes and integration that Te Whatu Ora will want, our recommendations all sit around four themes:

a) Architected for security: designing in data segmentation, identification of high risk/value data assets, the use of encryption for data, access controls, a monitoring and logging framework, and others. The design phase can limit damage in the event of an intrusion and make the system more resilient. At the same time, systems need to be usable at a clinical level, reflecting pressures and urgencies at the point of delivery. Highly secure systems will not be used if they are awkward, time-consuming or non-intuitive in practice;

b) Kept up to date: patching is the classic recommendation here. But for the healthcare system in NZ, it also means systematically investing to eliminate unsafe legacy systems, to make full use of well-managed cloud systems, and to accommodate the increasing use of internet-connected medical devices in a safe manner. It also means investing in people, both through IT skills and by providing clear frameworks for others: for example, a '**code of connection'** that sets minimum cybersecurity requirements for all parties and develop an assurance mechanism to ensure adherence, provide training and genuine support.

c) Active defence: Logging, monitoring, responding, planning. As noted above, this is a task for the whole system, including healthcare delivery colleagues at the clinical end. It cannot be left to IT teams. It requires the – otherwise excellent – CIMS framework to be updated. And it needs to be accompanied by the sort of behavioural discipline described above, otherwise it will fail; and

d) Practice. Every single person we have spoken to has enthusiastically endorsed the idea that cyber responses need to be rehearsed. "Train hard; fight easy" is more than a truism. Finding the time, and space to do this is always hard, especially in busy hospitals with real people to treat. But the costs of not doing so are very high and very unpredictable. The solution may be a 'simulator' – a national virtual IT resource to allow clinicians and managers as well as IT teams to practice for disruption in a virtual environment. It would also allow NCSC to simulate various types of attack, and better understand how to advise on the responses, without having to wait for the real thing. Results could be assessed from an equity perspective, as well as through clinical and technical lenses.

This structure of recommendations can be complemented by another, for the IT system design and operation teams themselves:

- To avoid and acknowledge the risks (getting design and operational protocols right);
- To detect and stop threats (logging, monitoring and responding – automatically where possible);
- To respond (limiting immediate impact when something gets through, as it will); and
- Restore.

None of this will be cheap: it will cost money and it will cost time, as managers and clinicians will need to be more involved. There is a real opportunity cost to that, which we acknowledge. But we see little alternative. The WDHB incident shows the level of disruption, the actual cost and impact on confidence that can accompany even a medium-sized intrusion. If we are to benefit from a national healthcare system, we need to be prepared to invest the time and money to make it safe in an unsafe world.

2 September 2022

9 APPENDICES

9.1 List of People Interviewed

Name	Position (At time of interview)
9(2)(k), 9(2)(c)	9(2)(k), 9(2)(c)
9(2)(k), 9(2)(c)	9(2)(k), 9(2)(c)
9(2)(k), 9(2)(c)	9(2)(k), 9(2)(c)
9(2)(k), 9(2)(c)	9(2)(k), 9(2)(c)
9(2)(k), 9(2)(c)	9(2)(k), 9(2)(c)
9(2)(k), 9(2)(c)	9(2)(k), 9(2)(c)

9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]
9(2)(k), 9(2)(c) [redacted]	9(2)(k), 9(2)(c) [redacted]

9.2 Acknowledgements

A lot of people worked to help us prepare this report, test its conclusions, and settle its recommendations. Those we interviewed more formally are listed above. Others made their contribution through the voluminous documentary evidence we received. We are grateful to everyone for the generous way people gave their time, especially as we unravelled some of the knottier challenges understanding the events after 18 May 2021. Thank you to you all.

It's sometimes invidious to single people out in a report which is very much a team effort, but we want to particularly acknowledge the contribution made by 9(2)(k), 9(2)(c), both during the incident and helping us make sense of it afterwards. His formidable intellect combined with a vital sense of perspective added immeasurably to our work.

And the InPhySec team too: Louise Kendall and James Collins each provided a rare mixture of technical and organisational insights and support.

9.3 Terms of Reference

Independent Review Terms of Reference: Health response to the Waikato DHB ransomware incident

1. Purpose

This review will provide advice to the Minister of Health, the Chief Executive of Waikato DHB, and the Ministry on what can be learnt from the Waikato DHB ransomware attack, vulnerabilities in the IT services and planning, and recommended actions that will minimise future risk and strengthen the cyber resilience of New Zealand's health and disability system.

2. Context

On the 18 May 2021, Waikato DHB suffered a ransomware attack which compromised IT services. The cyber-attack impacted many areas of the health services that the Waikato DHB provide to the community. The Waikato DHB stood up an incident response and the Ministry of Health provided national leadership to the incident, with input from other key agencies including the National Cyber Security Centre. The incident response focused on:

- Managing health service delivery.
- IT service restoration.
- Assessing privacy impacts and notifying impacted individuals as appropriate. Cyber security incident investigation and response

3. Scope

The scope of the review is on two areas to be assessed, evaluated and reported on. In addition, outcomes are provided to detail the purpose and objectives for each topic within the review.

The topics, details of what will be reviewed, and their outcomes are as follows:

- Waikato DHB risk assessment and controls prior to the breach
- Capability and level of resource: including experienced security staff performing security related governance, risk and compliance (GRC) tasks and operational security related tasks.
- Information management: Including the policies and procedures for classifying information assets, understanding the business service impact of data loss or service disruption, 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.

- Information security controls: implementation of industry standard security controls including such things as logical access controls, monitoring controls, change control, software update and vulnerability management, and platform resilience.
- Technical architecture: how the technical environment was designed and deployed to mitigate and manage security risks, including what stops a security event affecting other systems such as an entire DHB or the wider health sector. The review should include how future system changes are implemented as not to introduce new security risks or undo existing security controls.
- Governance: IT services risk management and reporting and KPIs, roles and responsibilities, budgeting and funding, governance, strategy and roadmap development, on-going security assurance, reporting scope and regularity to the DHB's senior leadership team and governors.
- Outcome: Identification of any cyber resilience vulnerabilities DHB had prior to the breach that can be mitigated in other DHB health and disability systems to strengthen the resilience of the sector.
- WDHB IT service restoration
- Governance and decision making: The governance and decision making that determined the process for prioritisation of IT services to be restored.
- Timeliness: The timeliness of the IT service restoration process was appropriate.
- Restoration: Evaluate supporting documentation relating to the planned safe restoration of servers.
- Awareness of risk: The level of awareness of the potential risk exposure and guidelines including staff working practices and operational security monitoring.
- Expert assistance: The use of experienced experts to help ensure the restoration of services occurs quickly and without creating any further risk of another security breach.
- Outcome: Strengthen the process and mechanisms of IT service restoration within the health and disability system.

Out of scope

The scope of this review does not include:

- The criminal investigation of the cyber-attack.
- Attribution of any contributing factors to specific individuals involved in the incident.
-
-

Non-IT impacts of the breach, including how privacy was managed and or health service delivery impacts.

The overall response model, communications and engagement approach used to support response efforts

Concurrent incident responses (eg, NICU outbreak, COVID-19)

4. Stakeholders to be interviewed

The following organisations will be consulted as part of this review:

- Minister of Health
- Ministry of Health
- Waikato District Health Board
- Local Members of Parliament
- National Cyber Security Centre
- NZ Police
- Office of the Privacy Commissioner
- HealthShare
- 9(2)(k), 9(2)(c)
- 9(2)(k), 9(2)(c)
- Regional DHBs affected by the incident

Where the stakeholder's area of expertise is deemed out of scope of the review their interview will focus only on those items in scope as outlined in section 3.

5. Accountability

Group members are responsible for reporting back to (Minister of Health or other as required).

6. Review

The group review is to start the review post the recovery activities (estimate date February 2022 as confirmed) and complete by April 2022.

The review will be completed by an experienced member of the Department of Internal Affairs Security and Related Services panel.