New Zealand Medical Library Faces The Challenges Of A Cyberattack

Lyn Wood
Reference and Liaison Librarian | Te Whatu Ora Waikato
Lyn.Wood@waikatodhb.health.nz

Angela Broring
Library Manager | Te Whatu Ora Waikato
Angela.Broring@waikatodhb.health.nz

In 2021 our library team faced a new challenge – a cyberattack. We weren't reading about it happening somewhere overseas, we were living it. We have put together an account of how we managed our library services during a challenging nine weeks.

On 18 May 2021 the biggest ransomware attack in New Zealand occurred at Waikato District Health Board. Waikato District Health Board, subsequently known as Te Whatu Ora Waikato, provides secondary care across a geographical area of more than 21,000 square kilometers and serves a population of over 425,000 people. It comprises one major hospital in Hamilton and four rural hospitals as well as numerous rural healthcare centres. Over 8000 employees, including our team, use the same computer network (Te Whatu Ora Waikato, n.d.). On this day we were suddenly confronted with a total shutdown. Everything on the computer network was affected, including computers, phones, emails, appointment calendars, networked diagnostic machines, parking, security and even the EFTPOS in the cafeteria. We had no Internet, no intranet, no wifi at all. Patient delivery was significantly impacted - surgery was delayed and patients referred to other hospitals. As for the Library, there was no access to Library resources using the intranet – the main access point for most customers, and the library had no functioning desktop computers, laptops, printers, scanner or phones.

"I'm having trouble logging in, are you?"

May 18 2021 started like any other day, except, there was a glitch with the computers. We were logging in but nothing would open. Initial rumours were that this was a bad computer glitch and might take two days to fix. Later in the day it became apparent that we were facing a serious cyber attack and restoring computers would take at least a week. Eventually IS (District Health Board Information Service) "runners" delivered a message confirming that this was actually a serious ransomware attack and there would be no quick fix – and to "please stop trying to login to the computers".

It took nine weeks for the District Health Board to recover the computer network. As no ransom was paid it was a long, painstaking process of restoring all systems and files.

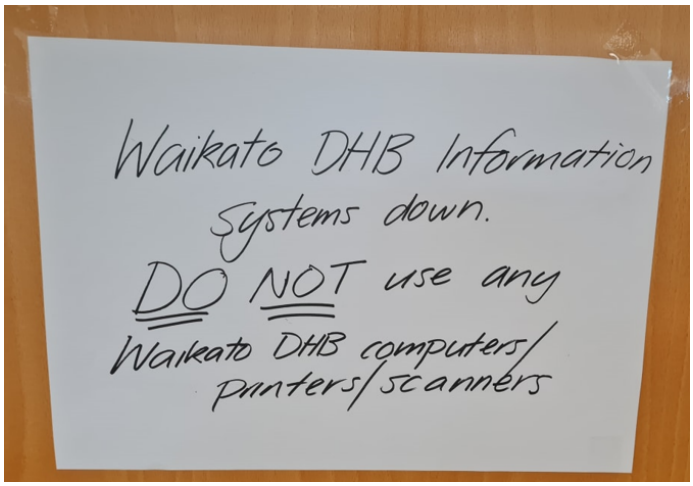
"What do we do first?" - signage

On that first day we were dealing with a barrage of customer queries – "Can I login?", "How can I print?", "How long will this last?" We needed signs to explain the situation. These signs had to be hand written as we could not use the printers. We could, however, make multiple copies of signs as the photocopying function of the printer/photocopier is not connected to the network. Despite signage some library customers were not deterred from trying to login to the computers. In the end we opted for removing the power cables to all computers.

Paper signs and notices continued to be an indispensable way to communicate to Library customers over the next nine weeks.

Figure 1

The sign used during the first week following the cyberattack. Press conferences regarding the cyberattack were held in the Library and the sign often featured briefly in news items.



Three essential e-resources identified, and the expired account dilemma

Within the first few days we became acutely aware that clinicians, pharmacists and nurses were struggling to find "non network" alternatives to access online resources - Lippincott Procedures, ToxINZ and UpToDate. Access to ToxINZ and UpToDate are critical for the hospital Pharmacy and the Emergency Department patient care services. Lipppincott Procedures is used across the organisation for patient care. Fortunately the Library supported "non network" alternative access to these resources. Both Lippincott Procedures and ToxINZ could be accessed using Open Athens (Library managed offsite portal or proxy service), Ko Awatea LEARN (learning/education portal), or directly with personal accounts. However, using

personal accounts is the only one "non network" option available to access UpToDate.

Setting up an UpToDate personal account requires customers to register on a work computer. Registering on a work computer provides IP authentication to authorise the account. Without access to work computers, no new accounts could be created. Only those who had accounts set up prior to the cyberattack now had access to UpToDate. An added complication to this access is that accounts expire within two months. To reactivate the account, the customer has to log in to UpToDate on a work computer, again for IP authentication to authorise the account. Many customers with personal accounts found they had expired or were soon to expire. The Library contacted UpToDate provider, Wolters Kluwer Health, about this dilemma and the two month period was extended to stop further accounts expiring. Unfortunately, the use of UpToDate personal accounts was not widespread so this action had minimal impact on improving accessibility to UpToDate.

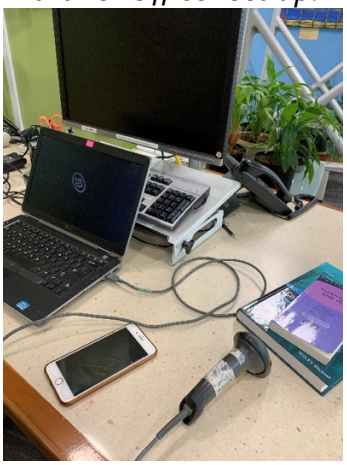
Setting up a parallel office and managing day to day services

Closing the library was never considered, probably as we never expected it would take so long to get back to normal. We just needed some temporary creative solutions. Fortunately our LMS (library management system), and all e-resources use offsite servers. We could effectively sidestep the the District Health Board network and intranet altogether. But we still needed computers.

While work desktops and laptops were unavailable we could use the two library iPads with SIM cards. Hotspotting data from personal phones gave us access to the Internet. Our LMS and other applications/e-resources were difficult to use on iPads so we managed to cobble together a more functional office using a motley collection of librarian's personal equipment; a couple of personal laptops, a home printer we could bluetooth to plus the personal mobile phones that were essential for Internet access.

Figure 2

"Parallel Office" set up.



With a personal laptop, hot spotting to a mobile phone, plus a library barcode scanner we had created a Circulation Desk (see Figure 2 above). We could issue and return books. There is no security risk using the scanner (nor using other plug in devices - keyboard, mouse, large meeting room screens). It was a relief to have this set up as we had a surge of customers visiting the library wanting to borrow books. Many customers, now unable to use computers, took the opportunity to catch up on reading our print collection. Customers continued to visit the library for resources and services. This was not surprising as without phones, email, or livechat, if you needed anything you had to walk to the library and ask in person! As the rest of the hospital were confronted with the same issues, there was a lot of walking between departments to communicate in person, use of personal phones and devices, and reinstating of old manual systems.

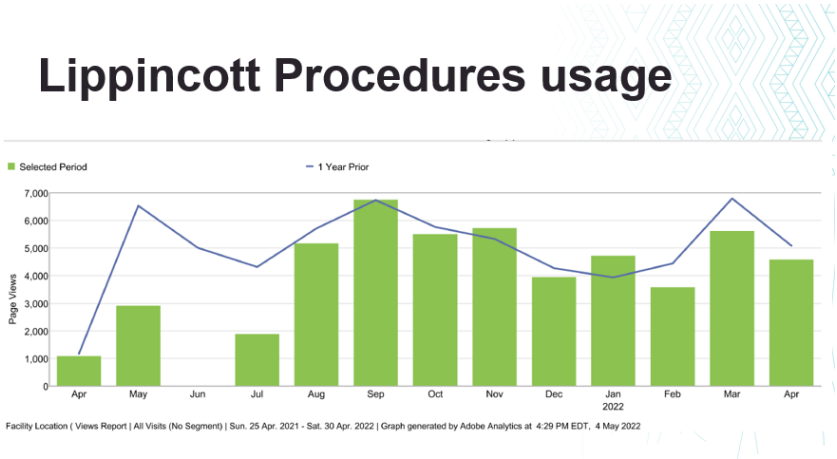
While our hastily assembled office allowed us to continue providing library services, it was not ideal. The decision was made to "turn off" supplying interloans to other libraries via OCLC and Te Puna. This allowed us to focus on providing a functional service to our customers. Medical librarians across New Zealand offered support to our library once they heard about the cyberattack. We appreciated the many offers of support.

Not being able to access our computer file system was a constant headache. Fortunately we had some key documents printed, in particular links to databases and login details, plus vendor contact details. It really helped having some critical information kept outside the computer network.

As customers could no longer search databases and access resources on work computers, our usage statistics for online resources dropped to a shocking low. As time went on, there were fewer requests for books, articles or literature searches.

Figure 3

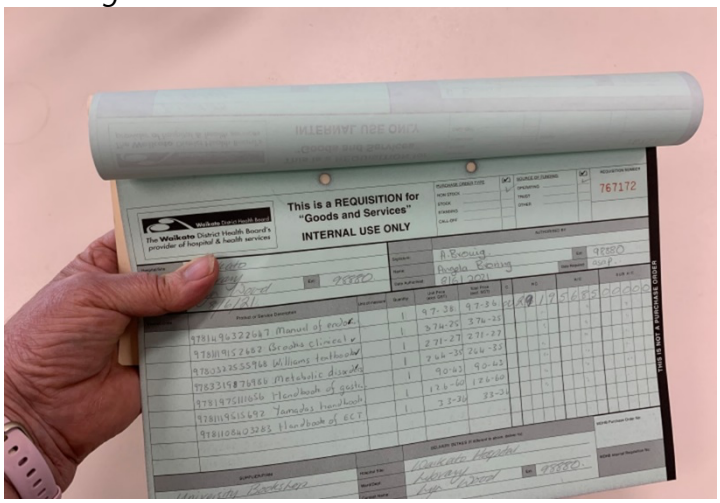
Lippincott Procedure usage showing a notable drop in use over May, June and July 2021



With the drop off in requests we realised we had an opportunity to use this time to tackle other tasks. The challenge was to find tasks that could be done within the limitations of our work environment. We began an acquisitions project, reviewing our collection and purchasing books. The District Health Board's Purchasing and Accounts Payable team were able to process orders again within several weeks of the cyberattack. Initially orders were "triaged", clinical first, but soon we were also able to submit orders.

Figure 4

Old manual systems were reinstated, including use of paper requisition forms for ordering new books



Using our parallel office did create an unexpected problem. We hadn't considered the ergonomics of our new work environment and two librarians experienced injuries associated with poor ergonomics.

Communication, emails and telecommunications

In the first few days following the cyberattack we desperately sought updated information, and guidance. To continue to provide library services we needed to know "what was going on" and the best way to respond. The Library Manager constantly sought the latest information to ensure our responses were on track. It was a priority to find a "non network" means to access work emails, our personal work accounts and the two generic Library email accounts. Access to our generic accounts was essential, not just to communicate with customers and vendors but also to access some online resources. These online resources required an authentication confirmation link or code that was sent to work email addresses as part of the login process.

We were more fortunate than many District Health Board employees as we were never without some access to work emails and MS Teams. Initially the Library Manager's mobile phone provided both access to emails and MS Teams. We would huddle around the Library Manger's phone to listen to the updates from the incident

meetings. In time we were able to set up email access for our team on iPads and personal devices.

While we could now use our work emails we had not anticipated how email recipients would respond to emails received from our organisation. Some email recipients would not open any email that "appeared" to be coming from our organisation for fear of risking a cyberattack happening to their own organisation. It did not help that Ireland's health system had also been attacked recently and everyone, including vendors, were on the alert and very security conscious. Realising this reluctance to engage in email correspondence we would first phone the recipient to explain that we were sending an email and that it was perfectly okay to open it.

Though essential critical phone lines were set up quickly within the District Health Board it was six weeks before the Library desk phones would be functional again. During this time we relied on the Library Managers phone or personal mobile phones.

"Applications that are back up and working and safe to use"

IS had quickly established wifi towers and safe, "green stickered", computers to use in critical areas of the hospital. It was then a gradual process of checking and reinstating computers across the District Health Board. The Library was not considered a priority and the Library Manager had a critical role advocating for restoring our Library computers as quickly as possible. Eventually the Library received a wifi tower, which meant we no longer had to use personal mobile phone data to keep our parallel office functioning. Then finally the Library computers were restored. Six weeks after the the cyberattack we had access to a small range of applications and resources, and a limited intranet on computers – although this did not look anything like pre-cyberattack computer access.

Over time, and according to priority, critical clinical applications were restored. From June onwards we received regular updates on restored and "next to be restored" applications. At this time most links on the Library intranet page were not working. We would alter our Library signage to inform our customers which applications were available.

The availability of MS Teams on computers presented an opportunity for hospital departments, including the Library, to use this as an access point for online resources, policies and guidelines. But as more of the Intranet and library e-resources became available on work computers this too, like our motley collection of office equipment, became redundant.

Whitelisting

IS continued to restore applications and began cautiously whitelisting websites. A whitelist (allowlist) is a cybersecurity strategy that approves a list of email addresses, IP addresses, domain names or applications, while denying all others. Only explicitly whitelisted websites could be accessed from the District Health Board's computer network. Ordinarily the organisation's employees accessed approximately 100,000 different websites every month so managing the whitelisting was a huge task. We had prioritised our list of 27 library resources for whitelisting, with UpToDate at the top of the list. UpToDate was whitelisted six weeks after the cyberattack. We promoted the access across the organisation and around the library. Eventually all the point of care tools and databases became accessible from work computers. But there were other websites that needed whitelisting to enable us to get closer to offering our normal services, our LMS, OCLC, OpenAthens administration site, book vendor sites, the list seemed endless. While customers could now search the Library databases the articles found in the databases were often, frustratingly, blocked. It was a long drawn out process to identify the many different publishers website domains that needed to be whitelisted. The term whitelisting became part of the librarian vernacular. In July, IS were able to open access to all websites in the "health" category and then later "education" category, this significantly reduced the task of identifying all the individual websites needing whitelisting. Whitelisting took many weeks but nearly brought us back to normal, though every now and then another failed attempt to access an article or a website identified another website domain to be whitelisted.

The lessons we learnt from this event

Importance of networking and the role of advocacy

- Restoring Library services is not a priority in the event of a computer network failure in a large health organisation, it's necessary to lobby for support.
- Regularly connecting with colleagues across the organisation will enable you to gain useful insights and practical tips.

Value of "non-network" access

- Set up access to emails on multiple devices that operate outside the computer network.
- Personal accounts allow access outside the network. It is essential to keep these current in case of unexpected events. DHB employees should be encouraged to create personal accounts to online resources they regularly use.
- Apps require personal accounts and provide user friendly access on network independent devices. Ensure all Library network independent devices have working apps.

- An alternative portal access is invaluable. Proxy servers Open Athens and EZProxy are independent of the network. All our Library e-resources, except UpToDate, are accessible by Open Athens.

Access to essential information

- Make sure all logins and web links to databases are updated and you store the information outside the computer network.
- Keep vendor details up to date and accessible and stored outside the computer network, possibly a printed record.

Importance of teamwork and finding creative solutions

- Think outside the box. Explore the potential of everything available to help keep the Library operational.
- Be mindful of the impact of the new work environment on staff wellbeing e.g. workplace ergonomics.

Cyberattacks are on the increase. The criminals responsible are innovative and we live in a constantly evolving environment of risk. An investigation of the cyberattack on our organisation lead to recommendations concerning security measures for the wider Te Whatu Ora Health New Zealand. Your organisation will have security measures in place to reduce the risk of a cyberattack but it might be useful to consider how your Library would respond should you face a cyberattack.

References

Te Whatu Ora Waikato (n.d.). Snapshot of Te Whatu Ora Waikato. https://www.waikatodhb.health.nz/about-us/snapshot-of-waikato-dhb/

Further reading

Hoffman, T. W., & Baker, J. F. (2022). Navigating our way through a hospital ransomware attack: Ethical considerations in delivering acute orthopaedic care. Journal of Medical Ethics, medethics-2021-107876. https://doi.org/10.1136/medethics-2021-107876

Stokes, A. M. (2022). Disruption of library services due to hospital cyberattack: A case study. Medical Reference Services Quarterly, 41(2), 204-212. https://doi.org/10.1080/02763869.2022.2054198

Waikato District Health Board ransomware attack. (2021, May 24). Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Waikato_District_Health_Board

Yap, M., Luo, A., Majumdar, A., & Singh, T. (2021). Maintaining the maxillofacial service under cyber-attack: The Waikato experience. ANZ Journal of Surgery, 91(12), 2566-2568. https://doi.org/10.1111/ans.17177