

UVM ScholarWorks

Disruption of Library Services Due to Hospital Cyberattack: A Case Study

Item Type	article;article
Authors	Stokes, Alice
Citation	Stokes, A. M. (2022). Disruption of Library Services Due to Hospital Cyberattack: A Case Study. <i>Medical Reference Services Quarterly</i> , 41(2), 204–212. 10.1080/02763869.2022.2054198
DOI	10.1080/02763869.2022.2054198
Download date	2026-05-08 14:38:36
Item License	http://creativecommons.org/licenses/by-nc-sa/4.0/
Link to Item	https://hdl.handle.net/20.500.14849/5929

Disruption of Library Services Due to Hospital Cyberattack: A Case Study

Alice M. Stokes

Dana Medical Library, University of Vermont, Burlington, USA

Alice Stokes, alice.stokes@uvm.edu, Dana Medical Library, 81 Colchester Avenue, Burlington, VT 05405, USA

Notes on contributors

Alice M Stokes, MLIS (alice.stokes@uvm.edu) is a Library Associate Professor and Research and Education Librarian at the Dana Medical Library, University of Vermont, 81 Colchester Avenue, Burlington, VT 05405, USA.

Disruption of Library Services Due to Hospital Cyberattack:

A Case Study

Abstract:

Cyberattacks on healthcare organizations increased dramatically in 2020 and 2021. The University of Vermont Medical Center suffered an attack in October 2020, during the second wave of the COVID-19 pandemic. The disruption to hospital computer systems had wide ranging impacts, including loss of online access to the medical library for nearly three months. Library staff worked to reduce impacts and increase access for hospital employees until full access was restored. This case study offers lessons learned and resources for health sciences libraries planning for a potential cyberattack.

Keywords: cyber-attack, cybersecurity, ransomware, healthcare, hospital, library

INTRODUCTION

In recent years, healthcare systems have been a common target of cybercrimes that seek to disrupt services and/or steal sensitive patient data for financial gain, including ransomware attacks and data theft.¹⁻³ Cyberattacks on healthcare organizations increased dramatically in 2020 and 2021.^{4,5} It was a particularly active time for cybercrimes in general, many of which used COVID-19 themes such as COVID-related domain names to exploit the COVID crisis. Technological adaptations in healthcare services and workflows during the pandemic, including a rapid pivot to telehealth and remote work, introduced new cybersecurity risks in the hospital setting.⁶ At least 239 million healthcare cyberattacks were attempted in 2020, an increase of nearly 10,000% from 2019.⁴ According to the Department of Health and Human Services, one of the

most noteworthy attacks in the United States in 2020 was the cyberattack on the University of Vermont (UVM) Medical Center in October 2020.⁴

The University of Vermont Medical Center is an academic medical center associated with the University of Vermont Larner College of Medicine and College of Nursing and Health Sciences. It is the community hospital for 168,000 people and the referral hospital for one million people in Vermont and New York.⁷ It is the only Level 1 Trauma Center in Vermont and houses the only children's hospital in the state. With 620 licensed beds, the hospital employs more than 8,800 people.⁷

The Dana Medical Library is the health sciences library for the University of Vermont and the University of Vermont Medical Center. Located in a concourse between the hospital and the medical education center, it serves the University of Vermont Medical Center, the Larner College of Medicine, the College of Nursing and Health Sciences, and the health sciences information needs of the broader university campus. Following the cyberattack on the UVM Medical Center, library services were substantially disrupted for hospital employees.

Because the Dana Medical Library is part of the University of Vermont Libraries, library systems reside on the university network. This had important implications during the cyberattack—some positive and some negative. Hospital libraries may be more vulnerable to complete disruption from cyberattacks than academic health sciences libraries. However, some of Dana Medical Library's experiences and lessons learned should be relevant to most health sciences libraries.

CASE STUDY

About the attack

Dana Medical Library staff first heard that there might be a disruption to the network at the UVM Medical Center on October 29, 2020, when it was reported in the news.⁸ The library did not receive any notification from the hospital directly, because all computer systems were taken offline as soon as the problem was apparent. When UVM Medical Center Information Technology (IT) realized that there was a widespread problem, they shut down the internet and electronic health records (EHR) system to prevent further infiltration.⁹

The attack downed the phone system, cut off access to staff emails and medical records, and slowed the hospital's ability to provide radiation treatment and run scans. A few hours after the attack began, a message was discovered on a network computer that stated the data had been encrypted with information on how to contact the attackers. There was no specific ransom note or dollar amount. Hospital IT staff immediately contacted the FBI.⁹ No effort to contact the attackers was made and no ransom was paid.¹⁰

All hospital computer systems were down for several weeks. Electronic health records were inaccessible. Staff returned to using paper charts and many patient appointments were canceled. Essential hospital services continued, but in the early days of the attack only half of scheduled procedures and operations were performed.¹¹ While there was significant disruption to hospital services across the board, no data was breached in the attack. During this period, UVM Medical Center furloughed and reassigned more than 300 employees in response to the effects of the attack.¹²

The hospital IT team wiped all servers clean and rebuilt them, and wiped and reimaged 5,000 laptops and computers. The Vermont National Guard Combined Cyber Response Team was brought in to assist with this process, providing essential technical assistance and personnel.¹³ It took 25 days to restore access to the electronic health

records system, and longer to fully restore all systems.¹⁴ The attack was estimated to cost \$1.5 million per day, for a total cost of at least \$40 and \$50 million.^{10, 15}

What caused the attack?

Forensic analysis revealed that a hospital employee took a corporate laptop on vacation in October 2020 and opened a personal email from their homeowner's association that contained a "phishing" scam.¹⁵ When the email was opened, cybercriminals deposited malware onto the laptop. A few days later, when the employee returned to work and connected to the hospital network, attackers were able to use the malware to launch the network-wide attack. The hospital has since augmented its cybersecurity for all computers and the entire network, and increased training for employees on how to spot and avoid phishing attempts.

Library impacts

Hospital systems were down for approximately three and a half weeks, but it took nearly three months from the start of the attack to restore access for UVM Medical Center employees to Dana Medical Library systems (see Fig. 1)

[PLACE FIGURE 1 HERE]

LEGEND FIGURE 1. Timeline of cyberattack and recovery

The acute crisis at the hospital was resolved before Thanksgiving, but in early December library staff discovered that hospital employees still did not have direct remote access to the library and it took seven more weeks to get full access restored.

The hospital uses a client connector to hide hospital IP addresses from external sites, preventing IP authentication to library resources. Under normal circumstances, a special network connection between the hospital and the university allows the library's proxy server to bypass that restriction and provide access. As soon as the attack was detected, however, that special network connection was cut off. Users at the hospital could no longer access library resources. This took much longer to troubleshoot and fix even after the main hospital systems had been restored. It required the cooperation of many different parties. The medical library relationship with the College of Medicine was helpful in moving the process along.

Usual authentication methods were disrupted for most hospital employees. Like many academic medical centers, Dana Medical Library has a mix of hospital patrons who also have university credentials and those who only have hospital credentials. For those who had university credentials, the disruption was minimal, as they were still able to use the university proxy to access library materials. Those without university credentials had no electronic access to library services. Since medical center email addresses were not accessible for several weeks, and the hospital intranet was down, there was no way to communicate directly with hospital employees. This disruption to services included Interlibrary Loan (ILL), which usually uses UVM Medical Center email addresses as one of their screening tools for ILL access.

Library response

Throughout the disruption to library services for hospital employees, the library implemented a number of strategies.

- Flexibility: Interlibrary Loan accepted requests from users' personal email accounts

- Alternatives: The library encouraged users who had university credentials to use them, helped users set up individual accounts for databases that allow for remote access (e.g. UpToDate Anywhere), and encouraged patrons to physically come into the library to use the library's computers and internet to access resources
- Outreach: Once hospital email was restored, library liaisons sent messages to their departments outlining alternative access methods and resources
- Persistence: Library staff continued to work to fully restore access to library systems from the hospital network

DISCUSSION

Every library will have individual circumstances that determine how a hospital cyberattack impacts them. For Dana Medical Library, there were several mitigating and exacerbating factors. The main mitigating factor was that Dana Medical Library is part of the university side of the academic health center, so library systems were not directly affected. Library databases, subscriptions, servers, files, email etc. continued to operate without disruption.

The timing of the attack also reduced the impact on clinicians, because it happened at the beginning of the second wave of COVID-19 in Vermont. During this time clinicians were so busy with urgent patient care that librarians observed fewer requests for general literature, and most COVID-19 literature was open access. After an initial closure from March-August 2020, the physical library had reopened, so users had access to print and online collections in the library, which is adjacent to the hospital.

On the other hand, the biggest exacerbating factor was also separate systems. The library was protected from the worst effects of the attack, but it took much longer to restore the connection between the hospital and library because library IT systems and

services are separate. While library resources are important to hospital patrons, this was not the top priority for the hospital administration and hospital IT department coping with the dual crises of the cyberattack and COVID-19.

The timing of the attack also presented challenges. By the time essential hospital computer systems had been restored, in November 2020, Vermont was fully in the throes of the second wave of COVID-19. Library employees could not enter the hospital to visit departments or provide other in-person communication due to COVID-19 restrictions. Fewer hospital employees were entering or even passing by the library, so typical outreach options were reduced. Finally, difficulty in coordinating communication between the hospital, the library IT department, and the medical school IT department delayed the full restoration of access. If the library had been part of the hospital structure or the college of medicine, these barriers might have been reduced.

CONCLUSION

All health sciences libraries, especially those affiliated with a hospital or healthcare system, should be prepared for a cyberattack. Based on the Dana Medical Library's experiences, here are a few library-specific recommendations:

- (1) Develop a cyberattack plan. Review it regularly. Reflect upon and update the plan after any cyberattacks or cybersecurity incidents. (See resources in the Appendix)
- (2) Brainstorm alternative access options in advance of and during an attack. Some ideas that Dana Medical Library staff generated:
 - (a) Ask patrons for alternative contact information and add to library records, if possible
 - (b) Encourage users to set up personal accounts for databases when possible

- (c) Consider keeping key text in print, even when prioritizing e-books in your collection development plan
 - (d) Rethink current systems and restrictions: For example, consider temporarily accepting article requests from personal email addresses
- (3) Create a communication plan. Consider what options your library would have to communicate with patrons if usual methods (email, intranet, etc.) were cut off.

While no institution can completely eliminate the risk of a cyberattack, preparation can mitigate the impact on library services if one were to occur. Planning for this potential adverse event will benefit all health sciences libraries, and particularly those affiliated with hospitals or health systems. The author hopes that reading about this specific cyberattack and its impacts, other libraries and librarians can reflect upon and improve the readiness of their institution to respond to a potential attack closer to home.

Acknowledgements

The author would like to thank Lynda Howell, IT specialist at the Dana Medical Library, University of Vermont for her valuable input and feedback on this article.

REFERENCES

1. Martin, Guy, Paul Martin, Chris Hankin, Ara Darzi, and James Kinross. "Cybersecurity and Healthcare: How Safe Are We?" *BMJ (Clinical research ed.)* 358 (2017): j3179. doi: 10.1136/bmj.j3179.
2. Argaw, Salem T., Juan R. Troncoso-Pastoriza, Darren Lacey, Marie-Valentine Florin, Franck Calcavecchia, Denise Anderson, Wayne Burlison, et al. "Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks." *BMC Medical Informatics and Decision Making* 20, no. 1 (2020): 146. doi: 0.1186/s12911-020-01161-7.

3. Kruse, Clemens Scott, Benjamin Frederick, Taylor Jacobson, and D. Kyle Monticone. "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends." *Technology and Health Care* 25, no. 1 (2017): 1-10. doi: 10.3233/thc-161263.
4. Department of Health and Human Services Cybersecurity Program. "2020: A Retrospective Look at Healthcare Cybersecurity." (Report # 202102181030, Health Sector Cybersecurity Coordination Center (HC3), U. S. Department of Health and Human Services, Washington, DC, 2021).
<https://www.hhs.gov/sites/default/files/2020-hph-cybersecurity-retrospective-tlpwhite.pdf> (accessed February 14, 2022).
5. Luna, Raul, Emily Rhine, Matthew Myhra, Ross Sullivan, and Clemens Scott Kruse. "Cyber Threats to Health Information Systems: A Systematic Review." *Technology and Health Care* 24, no. 1 (2016): 1-9. doi: 10.3233/thc-151102.
6. Axel Wirth. "Cyberinsights: COVID-19 and What It Means for Cybersecurity." *Biomedical Instrumentation & Technology* 54, no. 3 (2020): 216-19. doi: 10.2345/0899-8205-54.3.216.
7. The University of Vermont Medical Center, The University of Vermont Health Network. "About the UVM Medical Center". Accessed February 14, 2022.
<https://www.uvmhealth.org/medcenter/about-uvm-medical-center>
8. Galloway, Anne. "UVM Health Network Investigating Apparent Cyberattack." *VT Digger*, October 29, 2020. <https://vtdigger.org/2020/10/29/uvm-health-network-investigating-apparent-cyberattack/> (accessed February 14, 2022).
9. Jickling, Katie. "FBI Is Investigating Cyberattack at UVM Health Network." *VT Digger*, October 29, 2020. <https://vtdigger.org/2020/10/29/fbi-is->

- investigating-cyber-attack-at-uvm-health-network/ (accessed February 14, 2022).
10. Jickling, Katie "Cyberattack Cost UVM Medical Center \$1.5 Million a Day." *VTDigger*, December 8, 2020. <https://vtdigger.org/2020/12/08/cyberattack-cost-uvm-medical-center-1-5-million-a-day/> (accessed February 14, 2022).
 11. Jickling, Katie and Mark Johnson. "Hospitals and Patients Scramble in Wake of UVM Medical Center Cyberattack." *VTDigger*, October 30, 2020. <https://vtdigger.org/2020/10/30/hospitals-and-patients-scramble-in-wake-of-uvm-medical-center-cyberattack/> (accessed February 14, 2022).
 12. Jickling, Katie. "300 Workers Reassigned or Furloughed at UVM Medical Center Due to Cyberattack." *VTDigger*, November 2, 2020. <https://vtdigger.org/2020/11/09/300-workers-reassigned-or-furloughed-at-uvm-medical-center-due-to-cyberattack/> (accessed February 14, 2022).
 13. Jickling, Katie. "National Guard Cybersecurity Team Deployed after UVM Medical Center Hack." *VTDigger*, November 4, 2020. <https://vtdigger.org/2020/11/04/national-guard-cybersecurity-team-deployed-after-uvm-medical-center-hack/> (accessed February 14, 2022).
 14. Jickling, Katie. "A Month after Cyberattack, UVM Medical Center Restores Access to Electronic Records." *VTDigger*, November 23, 2020. <https://vtdigger.org/2020/11/23/a-month-after-cyberattack-uvm-medical-center-restores-access-to-electronic-records/> (accessed February 14, 2022).
 15. Benninghoff, Grace. "Malware on Employee's Company Computer Led to Cyber Attack on UVM Medical Center." *VTDigger*, July 21, 2021. <https://vtdigger.org/2021/07/21/malware-on-employees-company-computer-led-to-cyber-attack-on-uvm-medical-center/> (accessed February 14, 2022).

Appendix

Selected resources for healthcare cyberattack awareness, preparedness and planning

American Hospital Association <https://www.aha.org/cybersecurity>

CDC <https://www.cdc.gov/cpr/readiness/healthcare/documents/healthcare-organization-and-hospital-cyber-discussion-guide.pdf>

HHS405(d) Aligning Health Care Industry Security Approaches
<https://405d.hhs.gov/public/navigation/home>

HHS Health Sector Cybersecurity Coordination Center
<https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html>

FBI <https://www.fbi.gov/investigate/cyber>