Summer 7-1-2024

Knowledge Held Hostage: What the British Library Ransomware Attack Can Teach Us

Moira Fiscus
moira.fiscus@siu.edu

Recommended Citation

Fiscus, Moira. "Knowledge Held Hostage: What the British Library Ransomware Attack Can Teach Us." *College and Research Libraries* 85, No. 5 (Summer 2024): 628. doi:https://doi.org/10.5860/crl.85.5.628.

Knowledge Held Hostage:
What the British Library Ransomware Attack Can Teach Us

Abstract: The British Library hack and its response serve as a clear example of the vulnerability of institutions of higher learning to such attacks and the importance of maintaining an open dialogue with the public during recovery. This open dialogue is currently lacking as universities attempt to move on and cover up these attacks quickly. This paper aims to start the conversation by providing three examples of institutions that went through a hack that left their services down for a significant period, how it affected those they serve, how these institutions responded, and what information was made public.

The British Library, a crown jewel among libraries with its long history and extensive collections, is a vital resource for researchers worldwide. In an event that is becoming dishearteningly common, this source of research materials was imprisoned on October 28, 2023, by a ransomware attack that saw the website, including staff emails, forced offline. For over two months, the British Library had no online presence and limited services in person. The first signs of recovery came on January 15, 2024, when an online viewable catalog came back but it still required researchers to come in person to review materials.(*British Library to Restore Access to Main Catalogue on 15th Jan after Cyberattack Outage*, 2023) Over 5 months later, recovery continues.(Keating, 2023)

Most frustratingly, the British Library happens to have the only extant copy of a sound recording I need for my research. My efforts to access this recording have taken a long and winding path and leave me wondering how universities or colleges have handled or could handle situations like what the British Library is experiencing. Half of my undergraduate education—the half with the heaviest research, of course— took place during the pandemic lockdown. This led me to select less fulfilling research topics dependent on what my library's limited physical and digital collection had available. What books and articles I could find formed the research nest that I stacked precariously around my workstation. I lived in that nest until the end of the quarter.

Now, as a new faculty librarian at another institution, I began this gathering process again. This time however, I could research what I wanted because I had the backing to access a full array of both physical books, online materials, and whatever else I wanted. When I started collecting the twigs for my metaphorical bird’s nest, I knew I could finally obtain one of the twigs that had eluded me during the COVID-19 lockdowns: a recording housed in the British Library of an interview with one of the founders of an organization I have been obsessively researching for years.

How hard could it be? Simple, surely? The groans from my librarian colleagues in interlibrary loan began the moment they learned of my simple plan and received my request. It turns out, those were the groans of experience from trying to get items from the British Library.

The next six weeks were filled with emails back and forth from my institution's Head of Access Services and myself to the British Library gatekeepers after they rejected our formal request for access to the recording. We received two different replies with two differing explanations of British Library policy regarding the loan of sound recordings, both of which were also different from the policy stated on the website. After my colleagues and I were very annoyed at the lack of proper communication, all parties finally agreed on the actual policy and we were then told the request could not be continued without obtaining copyright permission for

the recording. The National Trust, who own the rights, gave their permission and we relayed this happy development to the British Library.

The reply arrived a mere minute later, never a good sign when there is a six-hour time difference and since it was well past business hours in London. The Sound Archive staff declared they were unavailable for three weeks and would get back to us when they returned. Due to my request going through back channels rather than the formal interlibrary loan process, there was some additional logistical back and forth. We appeared all set and the recording would be sent at the beginning of November after processing on both ends.

Then, on October 28, the British Library was attacked by Rhysida, a hacker group that uses ransomware to take institutions hostage.

The attack locked both distant researchers and British Library staff out of all of their computer systems: from the online catalog to their own email accounts. Accessing anything within the library's enormous collections, both physical and digital, became nearly impossible and dependent largely on offline indices and hoping the tomes remained accurate after disuse. This brought to a standstill research by both those who traveled to London to view the collection and remote researchers like me who rely on digital copies.

While I can wait as the British Library works to untangle themselves and recover their trapped digital artifacts, it does leave me questioning how attacks like this happen and what I can do as a librarian if something like this impacts my library. How can I support students who need materials from our physical and print collections? With the British Library down and my research project in a holding pattern, I decided to look at other institutions and investigate their experiences with hacking to see what comfort, or discomfort, and lessons I can take from them. But first, for this cyber security illiterate librarian, what actually hit the British Library?

The answer is a type of malicious software called ransomware. Ransomware usually exploits a hole in an institution’s security to effectively freeze access and often steal data. Hackers using ransomware usually target employee or student information stored by the institution. Such attacks cause disruptions to services until the hacker group is paid a ransom to decrypt the trapped data or another means of decryption is found and employed. Payment may result in the restoration of services, but this is not guaranteed, and some cyber-security experts and the FBI do not support paying ransoms due to the lack of guarantees.(*Ransomware*, n.d.; Schell et al., 2019, pp. 118–119 & 141)

With the October attack, the British Library joins an ever-growing group of institutions of higher education and libraries being targeted by hacker groups hoping to extort ransom. Universities and colleges hold mountains of valuable data hacker groups want, especially student and staff personal information such as names and social security numbers. Compared to banks and large corporations, educational institutions have limited resources to address cybersecurity issues. This makes them attractive targets for hacker groups to target.(Coffey, 2023) To illustrate, the Cybersecurity and Infrastructure Security Agency (CISA), a U.S. government organization that promotes cybersecurity and investigates cybercrime, released a 2021 trends report that found that cybercrime and ransomware attacks have shifted from so-called “big-game” corporate targets, such as Colonial Pipeline, to smaller less protected targets. The CISA’s United Kingdom equivalent reports the biggest hacking target is the education sector.(*2021 Trends Show Increased Globalized Threat of Ransomware | CISA*, 2022) A separate advisory by CISA on the hacker group Vice Society, who primarily targets K-12 schools, laid out what can happen to

institutions of higher education if targeted by a cyber-attack, ranging from the delay of exams and canceled classes to stolen student data being sold or exposed to world (*#StopRansomware*, 2022) For example, in 2023, the University of Hawai'i paid a ransom after a community college in their system got hacked to prevent their student data from being sold on the dark web and, in their press release about the hack and the payment, stated that "64% of colleges worldwide reported experiencing some sort of ransomware attack, along with about 2,000 K–12 schools in the U.S".(News, 2023) The University of Hawai'i paid the ransom and, in what will be a trend, it is unclear if the payment worked the way they wanted, if recovery was better, and if no private data got put online. While The University of Hawai'i was open that they paid the ransom, in almost a year there have been no further updates. The amount of institutions of higher learning getting attacked is only likely to grow as ransomware groups continue to profit through ransoms paid or data sold or both.

Another reason to target the higher education sector is the way the basic ideals of higher education, such as academic freedom and equal access to knowledge for all those connected to the institutions, leave many openings for hacker groups to exploit(Mcginn, 2017) Unless higher education abandons the idea of equal access, which absolutely should not happen and is incredibly unlikely to without a fight, these practical holes are here to stay. Steps to narrow those openings and protect institutional servers and data can and must be taken, however.

Finding information about protections against ransomware and plans for IT address an attack once one is detected is straightforward once you start looking. Harder to find is information on what effects a hack would have on research and education. As an outsider, all you can see are glimpses.

During the Summer 2023 semester, students at Stephen F. Austin University were unable to do any assignments due to being locked out of their online learning programs for 10 days while the school worked to restore online access. Students, professors and staff were also unable to access their emails leaving online students unable to contact professors or other students, some professors and students resorted to using Facebook. Professors also needed to adjust their courses to recover lost time.(McGee, 2023) Ten days during the fast-paced summer term is a huge disruption. Students suffered both the leak of their personal information and the interruption of their education.(*SFA*, 2023)

In September, 2021, Howard University experienced an attack on a smaller scale compared to Stephen F. Austin University and the British Library which limited access to their online resources, resulting in the cancellation of online and hybrid classes for a few days.(Ngo, 2021) Reports weeks after the initial hack indicated frustration among students with the unavailability of internet connectivity for several days on campus, the lack of feedback on assignments, and the inflexibility of professors who required students to submit assignments on time, without feedback or easy access to the internet to use the Blackboard course management system. Students voiced their frustration to reporters in the weeks following but then the story died, partly due to systems coming back online and because Howard University, much like Stephen F. Austin, appears to have said very little in the weeks and months after.(Collins, 2021; Musungira, 2021)

As an outsider reading about these incidents, there seems to be limited follow-up. Stories stopped appearing in the news soon after the incidents happened and there was little public comment by faculty or staff. How did the hack affect the academics of students? What lessons

were learned by the people handling the incidents? This lack of comment seems to be a common theme when examining cyberattacks on higher education.

The exception to this trend is Regis University in Denver, Colorado, which experienced a hack in 2019 during student move-in that left parts of their system inaccessible for two months and caused continued issues in the day-to-day operation of the university even after Regis paid the ransom. In the meantime, students reverted to using paper for assignments.("Denver's Regis University Paid Ransom to 'Malicious Actors' behind Campus Cyberattack," 2020; *Nearly 2 Months after Regis University Cyberattack, Officials on Denver Campus Still Trying to Recover – The Denver Post*, 2019; *Regis University Paid Ransom after Cyberattack Last Fall*, 2020) The spokeswoman for Regis spoke regularly to a *Denver Post* reporter into 2020 and Regis maintained a blog with updates about the restoration of their online services. This goes beyond what has been seen at some other universities with Regis maintaining a clear line of communication with its students, the public, and potentially any alumni that wanted to monitor the situation.

When an attack like those that struck Regis and the British Library happens, the fix is not as simple as merely restarting the system. You pray your institution has a good backup from which to rebuild or your institution will be left to start again from scratch because if you use what was hacked, there is no guarantee that it is free of lingering malware[1]

Prior to the British Library hack, Regis provided the best example to other higher education institutions by sharing their story to help others learn from their experience and mistakes. Today, courses related to cybersecurity taught at Regis include lessons learned from the attack. Regis also held a summit that gathered interested parties from across the region to discuss the cyberattack and methods to prevent or recover from.(*Regis University Paid Ransom after Cyberattack Last Fall*, 2020) Even with all the information shared by Regis, there remain gaps such as student support efforts and effects on student learning. While reports from Howard, Stephen F. Austin, and Regis described initial student reactions, documentation of long-term effects is missing. This could be a result of how recently some of these attacks occurred, but it should be something we are mindful of in the future to learn how best to help students.

Prevention is currently the best way to protect students from disruptive cyberattacks. While it can feel like there is nothing we can do as individuals to stop someone else from opening a suspicious email and unleashing torment on our campuses, there are steps we can take. We can support IT, both in educating ourselves and in supporting campus-wide training to teach how to spot and deal with a suspicious email. This type of training should go beyond the typical orientation new students and faculty receive on their arrival and should include up-to-date prevention techniques.(Schell et al., 2019, pp. 135–137) This training needs to be encouraged and required by top administrative officials so those lessons are not ignored.

By way of example, my institution participates in yearly state-mandated cybersecurity training that teaches every university employee the signs of a suspicious email and how clicking a link in those suspicious emails could result in a hacker group compromising our system. The next week, we must complete sexual harassment prevention training. Notice of this training arrives in our email inboxes from an unknown and strange address with the subject line "Urgent"

---

1 (*Nearly 2 Months after Regis University Cyberattack, Officials on Denver Campus Still Trying to Recover – The Denver Post*, 2019)

and includes several other indicators of suspicious emails sent by hackers described in the cybersecurity training of the previous week despite linking to legitimate training materials we are required to complete. Ironically, this proves how effective that yearly cybersecurity training courses is, as several of my colleagues did not open that email and reported it to campus IT as a potential threat. This is the correct response. If an email meets all the hallmarks of being sent from a hacker group or other scammer: do not open it! The best way to protect students from a lengthy cyberattack outage is to prevent it from happening.

If an attack does succeed, it is important not only to quickly rebuild our systems but also to learn everything possible from it. In an interview about the hacks at Regis and another college, solutions architect, Christian Schreiber, stated that "victims of attacks like ransomware often focus on containing the damage and returning to normal operations as quickly as possible rather than conducting a detailed (and expensive) investigation into how the attack occurred."(McKenzie, 2019) This can leave institutions open to further attacks. Another way is to learn from other times the unexpected affected students, such as weather that leaves campuses without power and access to the internet or a global pandemic that blocks access to physical collections.

As the threat of hacking continues to haunt institutions of higher learning and education, not only do we have to work at actively preventing these attacks but those who have experienced a hack should share what lessons they learned and how they helped their students and staff during that time so others can add to it and prepare themselves. That is where a lot of institutions have failed, once a hack happens, they either work at recovery or in the case of Lincoln College in Illinois throw in the gloves and close after successive administrative issues(Nietzel, 2022) and then never discuss it. That is why the story of Regis is such an interesting one, because while researching this story it appeared that Regis was either the only or most noteworthy university to explain what happened and how they overcame it. But even then, this appeared limited to a conference they organized, and the material, including slides, is either difficult to impossible to track down or is unavailable online. As a standard bearer for accessible information, of sorts, Wikipedia does not even mention the hack on Regis University's Wikipedia page. If a headline breaks about an institute of higher education being hacked, little follows it for the public. No follow-ups or reports. Even when information is given to the public is it piecemeal and unclear, with no follow-up. For example, the University of Hawai'i did not state if they had been in contact with the FBI as other universities had announced when facing a similar situation. It feels like these events happen and is handled only to then be forgotten and not learned from.

That was until March of this year when the British Library themselves released an 18-page report on their hack, additionally to the updates via their blog in the preceding months, which explained what happened, how it affected their services to the public, and how they were working at repairing their damaged system. The British Library has been better than any other institution of higher learning when it comes to communicating about their hack and recovery along with being significantly better at this than communicating about their interlibrary loan policy. Not only did they release a report for public consumption they have also been releasing updates explaining where in the process of recovery they are and plans for the future. The British Library has not buried information, has not moved on and kept quiet, they are open with what information they can share and are sharing, unlikely many of the examples given in this article. The report can also show what happens when IT departments are understaffed and under-

resourced as the British Library depended on outside sources of IT infrastructure which ultimately left them open to harm. This helps to reinforce the importance of a well-supported and well-paid IT staff. While the hack was harder to overcome and hide from than the universities mentioned in this article, the British Library has not ignored the public's interest in it. And yes, the British Library hack does have its own Wikipedia page. And unlike other hacks, reporters came in and reported how the British Library was operating under stress and how patrons were acting such as the wonderful report by Sam Knight in *The New Yorker* which detailed their experience getting a book from the British Library.(Knight, 2023) The British Library is a place of learning, just like a university and as time has moved on the more dependent on online services it has become and to be severed from these services would have the effect of sending the British Library back decades. Both libraries and universities have people with emotional, financial, and educational stakes and attachments and are governed by open communication and scholarship. There is a duty to share information that affects them with others and to be open about being attacked by hacker groups. While there is plenty of literature on what to do before a hack and how to overcome it from an IT perspective, there is a gap in what attacks against education and information mean for us as students, researchers, and a society. And this gap can create a scramble if not addressed.

As of 2021, the National Center for Education Statistics found that 40% of both two-year degree-seeking undergraduates and postbaccalaureate students along with 20% of four-year degree-seeking undergraduates exclusively took online courses.(*The NCES Fast Facts Tool Provides Quick Answers to Many Education Questions (National Center for Education Statistics)*, n.d.) These numbers were likely affected by the pandemic but do reflect the growing popularity of partial or completely online degrees within higher education. This translates into students being further away from campus, their professors, and their school's physical collections of research material. With this move toward online learning, being hacked like the British Library and unavailable for months puts students' learning in harm's way.

We need to learn from those who have recovered from cyberattacks and we need to be open about our own experiences without fear of reputational damage. If the British Library can share and be open with their patrons, universities can share and be open with their students and faculty. We need to know how to prevent hacking. Discussions of how our institutions will handle cyberattacks must happen in advance, including what pre-planning can be done, what should be undertaken at each administrative level, and what faculty should do in case of long downtime. If hackers are going to take advantage of higher education's openness to attack us, let us also use that openness to learn from each other in how to best support our students, faculty, and IT departments while we prepare our defenses for our own "cyberincident."

Bibliography

2021 Trends Show Increased Globalized Threat of Ransomware | CISA. (2022, February 10). https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a

British Library to restore access to main catalogue on 15th Jan after cyberattack outage. (2023, December 19). The Bookseller. https://www.thebookseller.com/news/british-library-to-restore-access-to-main-catalogue-on-15th-jan-after-cyberattack-outage

Coffey, L. (2023, July 27). *MOVEit Attack Signals Growing Cybersecurity Threats for Higher Ed*. Inside Higher Ed. https://www.insidehighered.com/news/tech-innovation/2023/07/27/moveit-attack-signals-growing-cyberthreats-higher-ed

Collins, S. P. K. (2021, September 15). *Howard University Gradually Bounces Back from Ransomware Attack*. The Washington Informer. http://www.washingtoninformer.com/howard-university-gradually-bounces-back-from-ransomware-attack/

Denver's Regis University paid ransom to "malicious actors" behind campus cyberattack. (2020, January 28). *The Denver Post*. https://www.denverpost.com/2020/01/28/regis-university-ransomware-cyberattack/

Keating, R. (2023, December 15). *Knowledge under attack*. https://blogs.bl.uk/living-knowledge/2023/12/knowledge-under-attack.html

Knight, S. (2023, December 19). The Disturbing Impact of the Cyberattack at the British Library. *The New Yorker*. https://www.newyorker.com/news/letter-from-the-uk/the-disturbing-impact-of-the-cyberattack-at-the-british-library

McGee, K. (2023, June 20). *Stephen F. Austin State University students grow anxious about falling behind as school reels from cyberattack last week*. The Texas Tribune. https://www.texastribune.org/2023/06/20/stephen-f-austin-state-university-cyberattack/

Mcginn, S. (2017, February 1). *Universities must take steps to protect against ransomware attacks*. University Affairs. https://www.universityaffairs.ca/news/news-article/universities-must-take-steps-protect-ransomware-attacks/

McKenzie, L. (2019, August 26). *Cyberattacks Mar Start of Academic Year*. Inside Higher Ed. https://www.insidehighered.com/news/2019/08/27/two-universities-targeted-hackers-just-new-school-year

Musungira, K. (2021, September 28). Howard University continues to investigate ransomware attack as classes resume. *The Wash*. https://thewash.org/2021/09/28/howard-university-continues-to-investigate-ransomware-attack-as-classes-resume/

Nearly 2 months after Regis University cyberattack, officials on Denver campus still trying to recover – The Denver Post. (2019, December 19). https://www.denverpost.com/2019/10/16/regis-university-cyberattack-update/

News, U. H. (2023, July 26). *Hawai‘i CC cyber attack resolved | University of Hawai‘i System News*. https://www.hawaii.edu/news/2023/07/26/hawaii-cc-cyber-attack-resolved/

Ngo, M. (2021, September 7). Howard University Hit by a Ransomware Attack. *The New York Times*. https://www.nytimes.com/2021/09/07/education/howard-university-ransomware.html

Nietzel, M. T. (2022, April 1). *Lincoln College In Illinois To Close After 157 Years*. Forbes. https://www.forbes.com/sites/michaeltnietzel/2022/04/01/lincoln-college-in-illinois-to-close-after-157-years/

Ransomware. (n.d.). [Page]. Federal Bureau of Investigation. Retrieved April 10, 2024, from https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/ransomware

Regis University paid ransom after cyberattack last fall. (2020, January 28). KUSA.Com. https://www.9news.com/article/tech/regis-university-paid-ransom-after-cyberattack/73-c21c241e-4349-4b0f-ae88-99a61ab69e21

Schell, B., Passi, K., & Roy, L. (2019). How U.S. and Canadian Universities and Colleges Dealt with Malware and Ransomware Attacks in 2016-2017. *Journal of Information System Security*, *15*(2).

SFA: Roughly 8,600 counseling records, 100 government-issued ID numbers taken in June cyberattack. (2023, July 18). Cbs19.Tv. https://www.cbs19.tv/article/news/local/sfa-roughly-8600-counseling-records-100-government-issued-numbers-taken-in-june-cyberattack/501-9f15d498-36c1-4419-9161-e7604b8833a2

#StopRansomware: Vice Society | CISA. (2022, September 8). https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-249a-0

The NCES Fast Facts Tool provides quick answers to many education questions (National Center for Education Statistics). (n.d.). National Center for Education Statistics. Retrieved December 20, 2023, from https://nces.ed.gov/fastfacts/display.asp?id=80