WORLD LIBRARIES

Volume 25

No. 1

2021 worldlibraries.dom.edu/index.php/worldlib |

Effectiveness of Privacy Policies: A Case Study of the Schaumburg Township District Library

Susan M. Gordon

Dominican University

ABSTRACT

This case study examines the importance of information privacy and evaluates the specific information privacy policies and practices of a large suburban library. This study is focused on the Schaumburg Township District Library (STDL), to see how they are successfully protecting

patron information. The purpose of this study is to illustrate how STDL is adhering to best practices in their policies by being in accordance with the American Library Association (ALA) privacy policies, to review what was learned from previous cyber-attacks and how STDL has prevented any further attacks, to look at how STDL continues to re-evaluate and update their policies, and to determine ways they can improve areas that affect information privacy, including current technology and staff training. The study utilizes STDL's publicly posted information, website materials, and staff interviews to review the strengths and weaknesses of the methods that are being used and to exhibit how STDL is continually working to improve and insure patron data privacy.

INTRODUCTION

Information privacy, also called data privacy, is usually associated with personal information stored on computers. When looking at this topic regarding libraries, a simple definition can be found in *Information Privacy Fundamentals for Librarians and Information Professionals*: "Information privacy is being concerned with establishing rules that govern the collection and handling of personal information." (P. Swire and K. Ahmad, 2012, as cited by C. Givens, 2015, p. 4). We live in a technology driven world; having a privacy policy is important in order to protect information privacy. Givens also states that "protecting information privacy is a professional imperative. If people are free to exercise their right to receive information, they must feel secure that their preferences are not being monitored and will not be subject to negative consequences" (p. 8). Privacy policies vary by country but are required by law in different ways throughout the world. Personal data is constantly being gathered, especially every time someone uses the internet, and this data is often collected or sold by data brokers. Privacy policies are needed in libraries to ensure the daily protection of patron information, which is why the ALA has laid out guidelines in the Code of Ethics (Figure 1) and the Library Privacy Checklist (Table 2). Outdated library privacy polices (or worse, the lack of policies) puts patrons and their information at risk; libraries may not have the necessary technology in place to

protect data from being misused by 3rd parties, or the library falling prey to phishing scams, hackers, or cyber-attacks.

The focus of this case study is the Schaumburg Township District Library (STDL). It is a large, multi-location suburban public library. According to its website[1], STDL serves approximately 130,000 residents in 5 surrounding cities and has more than 1,000,000 visitors per year. The purpose of this study was to evaluate the effectiveness of the privacy policies and procedures at STDL (both how they are written and how well they are followed), as well as to look at the strengths and any weaknesses that they might have and to suggest ways to improve their patron data protection. STDL has strong Privacy and Confidentiality Policies[2] that this study determined are in line with the ALA policies and guidelines. (see Table 1 for a comparison). However, even with top-notch servers with virus-scanners, anti-virus software, firewalls, data encryption, and other intrusion deterrents, STDL, like many libraries, did fall prey to a cyber-attack in the past and from this they learned what to do in order to keep it from happening again.

METHODOLOGY

Case studies focus on the research and analysis of a subject for a particular entity. They can provide data for evaluation and improvement, but they can also be difficult to replicate. For example, not all libraries have privacy policies and those policies can also differ based on the type of library being reviewed (e.g. private, public, corporate, or educational institution). This case study only focuses on one specific library, STDL, to examine the effectiveness of their current policies and how well they protect patron data. Because they are such a large public

[1] https://www.schaumburglibrary.org/about/about-us
[2] https://www.schaumburglibrary.org/about/policies/privacy

library, it is important that they are able to ensure effective information privacy for the community that they serve.

RESULTS

Based on information gathered from the STDL website, posted in-house and publicly, and from staff interviews, it is evident that STDL takes personal and information privacy very seriously. STDL has clear, detailed privacy policies, abides by the Illinois State Law[3] regarding confidentiality, they have methods in place to safeguard personal information, and they even have a Children's Privacy Policy. The following statement, posted on the STDL website, displays how STDL has the additional support of its library board as well: "The Board of Trustees of the Schaumburg Township District Library seeks to protect the privacy and confidentiality of all who use the library in the pursuit of free speech, thought and association. The Library Board respects and supports an individual's fundamental right to open inquiry without scrutiny by others."

Libraries, like other institutions or businesses that have a high volume of people (which means there are copious amounts of data running through them each day), can have security breaches that can affect or endanger data privacy. STDL is no exception. The staff and IT Professionals[4] that were interviewed provided detailed information regarding a cyber-attack that occurred at STDL several years ago, as well as how they dealt with it and what was learned from the experience. Malicious hackers seem to be one step ahead of security systems, and many

[3] 75 ILCS 70/1 – Library Records Confidentiality Act (retrieved from https://www.schaumburglibrary.org/about/policies/privacy).
[4] The "IT Professionals" prefer to remain anonymous. Therefore, they are only named by title on the Reference page.

libraries were being hacked (including The Library of Congress and even more recently, the U.S. Federal Depository Library Program.[5]) The information from this interview is worth noting:

"The infection point was from e-mail phishing attacks that infected a staff person's computer. The virus on the staff computer then proceeded to exploit vulnerabilities on the server to run another virus to encrypt all user writable files. [NOTE: The files themselves were not infected with a virus, just encrypted.] The creators of the virus didn't care about what was encrypted, just that people were willing to pay to decrypt whatever files the virus was able to access. In fact, that was how the virus was able to be so effective and difficult for the US Government to combat. Since the local virus only needed to contact the hacker's server "for a brief moment" to get an encryption key to use, it generated little network traffic. This in turn made tracing the hacker's servers difficult. We reviewed which servers actually had "irreplaceable" data and which could be completely re-built and the software re-installed. [Note: The decrypted servers were eventually recreated, and data scanned "to be safe" before being copied over.] After this review, we paid the ransom to decrypt the other servers. For some reason, the payment site limited payment to two servers per day, which made the process longer. My only thought is that they didn't want to be traced by law enforcement. Therefore, it took a couple of days to decrypt the servers. At the time, the only thing you could do was to pay the bitcoin ransom and count on the fact that the hackers didn't want to get a "bad rep" for not providing the correct keys (as this would cause others to not even try to pay them)." No patron or staff data was ever at risk of being stolen or exploited.

STDL learned many things from the cyber-attack and the IT Professionals stated that they made the following changes shortly after it happened:

[5] https://www.cbsnews.com/news/iran-hackers-briefly-deface-website-for-u-s-government-library-with-pro-iranian-message/

- Migration of on-premise e-mail server to Office365 – “during the attack we were using a locally hosted version of Exchange with a barracuda e-mail filter that only updated it signatures every couple of days. Office365 has better deeper security and Microsoft is constantly updating its attack signatures.”
- Newer version of Windows – “all infected servers were recreated using a newer version of Windows that had existing security exploits patched. More importantly, by this time, Microsoft was finally realizing just how insecure their servers were and began focusing on increasing the effectiveness of its Defender scanner & local Firewall for both clients & servers.”
- Terminal Server Isolation of the accounting server behind a private network – “Staff that are involved with using the library accounting system now utilize a terminal server to access it. This prohibits access to the VLAN by regular network clients.”
- Implementation of a multi-tiered back-up strategy:
    - Purchase of a VMWare back-up solution & 1st tier storage repository – “to allow for quicker recovery of data”.
    - Purchase of a secondary back-up appliance – “this allows us to have a copy of the back-ups that, while still on the network, is in a more difficult to reach VLAN. This would be used in case something happens to the primary version above. “
    - Purchase of a cloud back-up hosting service – “this allows us to have a physically remote copy of the back-ups in case something more severe occurs at the Library and all of the server hardware is compromised.”
- Blocking of all traffic from known “bad actor” foreign countries – “this prevents suspect network traffic from even entering or going to these countries. This would have allowed us to mitigate the encryption as the virus would not have been able to “phone home” to get the network key to encrypt the files with.”

- Purchase and implementation of Intrusion Protection/Detection Software module for the firewall – "this provides the Library more aggressive scanning of all traffic that enters the network for behavior."

Currently, STDL also protects patron privacy by clearing the servers of all saved patron files each night. Safety measures are important to STDL and are routinely budgeted for every year, although budget limitations are always a concern.

DISCUSSION

According to Stastica.com, the annual number of malware attacks worldwide in 2019 was 9.9 billion. While America's privacy laws are inadequate because separate privacy laws govern separate states, areas, and industries, Europe created a global privacy standard (GDPR) that the world recognizes.[6] This reminds us of how important information privacy has become. In the library setting, users face increased risks and challenges when libraries do not have sufficient, effective privacy protection policies in place. Library patrons need to feel safe, knowing that their computer usage, browsing habits, and reading preferences will not be tracked and their personal information will not be sold. (*STDL does give patrons an option to sign up and have their checkout history maintained for them, but it is password protected by the patron themselves.)

STDL uses Cisco Umbrella Cloud Enterprise Network Security which is a suite of layered security for its systems. They also use DeepFreeze on the hard-drives which was described by one of the IT Professionals as "like placing a virtual layer of saran wrap of the hard-drive with all changes/data being placed on top of the saran wrap. When the computer is rebooted (which is

[6] https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

at the end of a user session), the saran wrap (and everything on top of it) is deleted and a new layer is put on top for the next patron. This is vital to the Library as it instantly deletes all patron login information and downloads, so the next patron cannot "accidentally" stumble upon them". STDL also tries to maintain up to date versions of all of their software on patron computers as well as the library servers, they monitor network traffic and investigate any anomalies, and arrange for penetration testing for overall network security.

One issue with the STDL privacy policy is that it was created in 2009. However, a staff member reported that STDL is currently reviewing the draft of their new privacy policy which will be presented to the Library Board for approval this fall. And the current pandemic has created budgeting issues that has caused STDL to invest in new technology for drive-up service as well as new procedures and staff training for materials that patrons request by telephone, all while STDL received Board approval to generously give homeowners a $1.5 Million abatement on property taxes.[7]

Another concern is regarding staff training. STDL does a good job training its staff, but according to some staff members, seems to be a bit lacking when it comes to making sure all of the staff understand the importance of patron information privacy, especially the ones that work directly with the patrons.

LIMITATIONS and RECOMMENDATIONS

Individual case studies do have their limitations. Technology changes rapidly and information security measures can be costly to update; there is no way to know if STDL will be able to

[7] https://www.dailyherald.com/news/20200604/schaumburg-township-library-board-approves-15-million-property-tax-abatement

maintain their high level of information privacy or remain consistent over time. Recent budget cuts due to Covid19 will have to be factored into STDL's current overall budget and those in the coming years. An additional limitation is the slight level of uncertainty that comes with interviewing current personnel; employees can have biases or speak overly enthusiastically about their employer for fear of retribution. Case study analysis can also be subjective and difficult to repeat.

Looking at the information gathered in this study, a few recommendations can be made:

- STDL could benefit from providing more comprehensive and continuing information privacy protection training to their patrons.
- Ensure that all employees receive patron privacy training.
- Update privacy polices more often and as needed due to unforeseen issues (Covid19) that create new challenges in the way the library serves patrons.
- Encourage the Library Board to support the library IT department when updated equipment or software is requested.
- Administration should continue to advocate for both staff and patrons.

CONCLUSIONS

STDL is effective in the way that they have adopted the ALA Privacy Checklist and continue to work to improve their privacy policies and procedures. Information privacy policies are becoming increasingly more important as technology advances, in order to be able to protect patron data. Cyber-attacks have been on the rise over the past few years so large libraries with thousands of users such as STDL need to continue to be ready to prevent the attacks from occurring. One of the challenges of this case study was to identify specific areas that need improvement, since STDL is already following ALA guidelines and state laws pertaining to

internet safety, information protection, and patron privacy. (This can be seen in the comparison chart as well as in the information reported in staff interviews.)

Measuring the effectiveness of library privacy policies demands a close review of the standards that impact how well they are written, how well they are being taught and carried out, and ultimately how well the library is protecting the personal data of its patrons. The way that their information privacy policies are being adhered to allows the Schaumburg Township District Library to accomplish their mission of providing information, programs, and services to all ages in a friendly and safe environment.

REFERENCES

Admin. (2020, June 18). Privacy. Retrieved August 10, 2020, from http://www.ala.org/advocacy/privacy

Burgess, M. (2020, March 24). What is GDPR? The summary guide to GDPR compliance in the UK. Retrieved August 22, 2020, from https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Clement, J. (2020, June 23). Number of malware attacks per year 2019. Retrieved August 22, 2020, from https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/

Dcaldwell-Stone. (2020, February 14). Library Privacy Checklist - Overview. Retrieved August 20, 2020, from http://www.ala.org/advocacy/privacy/checklists/overview

Givens, C. L. (2015). *Information privacy fundamentals for librarians and information professionals*. Lanham, London: Rowman & Littlefield.

Haris, L. (2020, January 05). Hackers briefly deface website for U.S. government library with pro-Iranian message. Retrieved August 21, 2020, from https://www.cbsnews.com/news/iran-hackers-briefly-deface-website-for-u-s-government-library-with-pro-iranian-message/

Illinois Statutes Chapter 75. Libraries § 70/1. (n.d.). Retrieved August 22, 2020, from https://codes.findlaw.com/il/chapter-75-libraries/il-st-sect-75-70-1.html

Keeshan, C. (2020, June 04). Schaumburg Township library board approves $1.5 million property tax abatement. Retrieved August 22, 2020, from https://www.dailyherald.com/news/20200604/schaumburg-township-library-board-approves-15-million-property-tax-abatement

Organizing Your Social Sciences Research Paper: Writing a Case Study. (2020, August 6). Retrieved August 10, 2020, from https://libguides.usc.edu/writingguide/casestudy

Privacy Protection Interview with STDL Branch Manager [Personal interview]. (2020, August 10).

Privacy Protection Interview with STDL IT Director [E-mail interview]. (2020, August 20).

Privacy Protection Interview with STDL Systems Administrator [Personal interview]. (2020, August 10).

Rberquist. (2019, May 06). Professional Ethics. Retrieved August 21, 2020, from http://www.ala.org/tools/ethics

STDL Privacy and Confidentiality. (2009, September 21). Retrieved August 10, 2020, from https://www.schaumburglibrary.org/about/policies/privacy

Swire, P. P., & Ahmad, K. (2012). *Foundations of information privacy and data protection: A survey of global concepts, laws and practices*. Portsmouth, NH: IAPP.

APPENDICES

Table 1

COMPARISON CHART

ALA Privacy Checklist	STDL Confidentiality Policy
Create a policy that addresses the collection of user information. Such a policy should specify that the library is not collecting more user information than what it needs and that it is not keeping the personally identifiable information of users longer than what is necessary.	The library will not collect personal information from individuals using public access computers in the library and will not collect personal information from individuals visiting the library Web site from home.
Create a privacy policy that is understandable by a layperson.	The library is committed to protecting personally identifiable information.
Make sure the privacy policy is posted in the library where the public can see it.	*(Privacy Policy is posted in all 3 library locations.)
Ensure that the privacy policy includes information about what information the library is tracking, why, and for how long the data is kept.	Types of personal information collected: name, phone #, e-mail, DOB, library card # only to provide or improve library service.
Ensure that the privacy policy includes when user information can be shared and under what conditions.	The library will not sell, lease, or disclose confidential information to outside parties unless required to do so by law.
Destroy all paper records with user data, such as computer sign-in sheets.	The library will avoid keeping unnecessary records.
Ensure all existing security certificates for HTTPS/SSL are valid and create a procedure for revalidating them annually.	Ensures that contracts and agreements with providers of electronic resources reflect our policies and legal obligations.

Designate a Library Privacy Officer to handle requests for personally identifiable information of users from law enforcement officials and other third parties.	*(Not stated in current privacy policy but there is a policy in place. Requests are referred to the Library Director.)
Ensure there is a formal process in place to address breaches of user data directly under library control or maintained by third parties. The library should notify affected users when they become aware of a breach.	*(Not stated in current privacy policy but there is a formal process in place to address breaches.)
Encrypt all user data with secure algorithms in all network and application communications.	The library will have security procedures that protect against loss, destruction, and unauthorized access to your information.
Purge search history records regularly, ideally when the individual computer session ends.	The library will remove from computers daily: cookies, search histories, cached files, and other records of Internet use.
Purge circulation and interlibrary loan records when they are no longer needed for library operations. Any user data that is kept for analysis should be anonymized or de-identified and have access restricted to authorized staff.	The library will purge and shred outdated records and remove the correlation between personal information and materials borrowed once these items are returned.
Utilize HTTPS wherever possible.	The library has security procedures that protect against loss, destruction, and unauthorized access to your information.

Images and information retrieved from: from http://www.ala.org/advocacy/privacy/checklists/overview , https://www.schaumburglibrary.org/about/policies/privacy

Figure 1

ALA Code of Ethics

As members of the American Library Association, we recognize the importance of codifying and making known to the profession and to the general public the ethical principles that guide the work of librarians, other professionals providing information services, library trustees and library staffs.

Ethical dilemmas occur when values are in conflict. The American Library Association Code of Ethics states the values to which we are committed and embodies the ethical responsibilities of

the profession in this changing information environment. We significantly influence or control the selection, organization, preservation, and dissemination of information. In a political system grounded in an informed citizenry, we are members of a profession explicitly committed to intellectual freedom and the freedom of access to information. We have a special obligation to ensure the free flow of information and ideas to present and future generations.
The principles of this Code are expressed in broad statements to guide ethical decision making. These statements provide a framework; they cannot and do not dictate conduct to cover particular situations.

1. We provide the highest level of service to all library users through appropriate and usefully organized resources; equitable service policies; equitable access; and accurate, unbiased, and courteous responses to all requests.
2. We uphold the principles of intellectual freedom and resist all efforts to censor library resources.
3. We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted.
4. We respect intellectual property rights and advocate balance between the interests of information users and rights holders.
5. We treat co-workers and other colleagues with respect, fairness, and good faith, and advocate conditions of employment that safeguard the rights and welfare of all employees of our institutions.
6. We do not advance private interests at the expense of library users, colleagues, or our employing institutions.
7. We distinguish between our personal convictions and professional duties and do not allow our personal beliefs to interfere with fair representation of the aims of our institutions or the provision of access to their information resources.
8. We strive for excellence in the profession by maintaining and enhancing our own knowledge and skills, by encouraging the professional development of co-workers, and by fostering the aspirations of potential members of the profession.. Code of Ethics (PDF) http://www.ala.org/tools/ethics