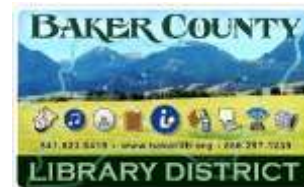


Baker County Library District
 Board of Directors + Contract Review Board
Regular Meeting Agenda
 Monday, Sep 9, 2019, 6:00 – 8:00 pm
 Riverside Room, Baker County Public Library
 2400 Resort St, Baker City
 Gary Dielman, President



- | | | |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| I. | CALL TO ORDER | Dielman |
| II. | Consent agenda (ACTION) | Dielman |
| | a. Additions/deletions from the agenda | |
| | b. Minutes of previous meeting | |
| III. | Conflicts or potential conflicts of interest | Dielman |
| IV. | Open forum for general public, comments & communications | Dielman |
| | In the interests of time and to allow as many members of the public an opportunity to speak, the board asks guests to limit remarks to five (5) minutes if speaking on behalf of an individual, or ten (10) minutes if speaking on behalf of a group or organization. | |
| V. | OLD BUSINESS | |
| | a. None | |
| VI. | NEW BUSINESS | |
| | a. Rivistas Subscription Services (ACTION) | Stokes |
| | b. Professional Audit Services (ACTION) | Stokes |
| | c. IT systems threat response | Stokes |
| VII. | REPORTS | |
| | a. Director | Stokes |
| | b. Finance | Hawes |
| VIII. | Next meeting: Oct 21, 2019 | President-elect |
| IX. | ADJOURNMENT | President-elect |

The times of all agenda items except open forum are approximate and are subject to change. Other matters may be discussed as deemed appropriate by the Board. If necessary, Executive Session may be held in accordance with the following. Topics marked with an asterisk* are scheduled for the current meeting's executive session.

ORS 192.660 (2) (d) Labor Negotiations
 ORS 192.660 (2) (h) Legal Rights

ORS 192.660 (2) (e, j) Property
 ORS 192.660 (2) (a, b, i) Personnel

Library Board Meeting – Annotated Agenda

Monday, Sep 9, 2019, 6:00 pm

Notes prepared by Library Director Perry Stokes

Annotated Agenda

- I. **CALL TO ORDER** Dielman
- II. **Consent agenda (ACTION)** Dielman
 - a. **Additions/deletions from the agenda**
 - b. **Minutes of previous meeting**

Attachments:

- II.b.i. Board meeting minutes, Aug 12 2019

- III. **Conflicts or potential conflicts of interest** Dielman
- IV. **Open forum for general public, comments & communications** Dielman

A local parent of a child with disabilities requested a meeting to discuss improvement project ideas. The meeting outcome is included in my Director reports.

- V. **OLD BUSINESS**
 - a. **None**

- VI. **NEW BUSINESS**
 - a. **Rivistas Subscription Services** Stokes

Attachments:

- VI.a.i. Rivistas BCLD quote for magazines
- VI.a.ii. Rivistas BCLD quote for magazines & newspapers

I am presenting this Personal/Professional Services Contract order for board approval. Per district purchasing policy, an informal competitive pricing process was used for selection.

BCLD Public Contracting Rules adopted 4/12/2010 provide that a “personal services contract totaling less than \$50,000 in either a calendar year or a fiscal year may be awarded by direct appointment, without competitive bidding. “

The District has about 310 periodicals subscriptions. This includes newspapers and magazines, for adults, teens, and children, at all branches, in English and Spanish. To save staff time and District funds, this fiscal year we will begin contracting with a subscription agent to purchase and manage delivery of the vast majority of subscriptions. This allows us to pay a single invoice for several titles rather than having to deal with hundreds of separate invoices. We also receive an 18% discount on magazines made possible from bulk purchasing by the agent and have a centralized software tool to report problems with missing issues.

After obtaining written quotes and service reviews of three vendors last fall with Serials Specialist Sylvia Bowers, we have selected Rivistas to be the district’s contract agent beginning this fiscal year. The cost is reasonable and the company has excellent service reviews from Sage partners and other libraries.

Library Board Meeting – Annotated Agenda

Monday, Sep 9, 2019, 6:00 pm

Notes prepared by Library Director Perry Stokes

Rivistas has provided two quotes, one for magazines only and another for magazines plus newspapers. Discounts from the magazine quote will save the district about \$1,200. Newspapers offer no additional discounts, so savings of staff time would be the primary benefit of including them.

BCLD - FY18-19 periodicals expenses	\$13,870
BCLD - FY19-20 periodicals budget	\$13,000
Rivistas - Magazines only	\$5,907.05
Rivistas - Magazines + newspapers	\$9,854.81

I request authorization of the Magazines + Newspapers order for \$9,855.

b. Professional Audit Services (ACTION)

Stokes

Attachments:

- VI.b.i. To be shared in meeting

Per board direction given at the August meeting, Christine and I released an RFP for Professional Audit Services on 8/21/19 with a response deadline of 9/6/19. Local and regional CPA firms were identified and directly contacted with an invitation to bid. Guyer & Associates were informed that the district would accept their engagement letter already provided as a bid but they were welcome to submit revisions.

At the meeting, Christine and I will present the competitive bid(s) received for board consideration and approval.

c. IT systems threat response

Stokes

Attachments:

- VI.c.i. CBS News – [Ransomware attacks on the rise – and small towns are in the crosshairs](#)
- VI.c.ii. Various ransomware articles

With a spike of ransomware attacks on small governments, including public libraries, I have insisted on a review of cyber protection and backup protocols by both BCLD and Sage system administrators. This agenda item is for board training about the severity of the threat and district actions and resources for combating it.

In Kentucky, Daviess County Public Library reported that

“At the end of this fiscal year, the library encountered a ransomware attack on its staff server. On April 28th it was discovered that a significant portion of our staff server had been encrypted and was being held ransom by an unknown source. DCPL did not pay the ransom. The server had to be reset and data needed to be restored. The Library was unable to restore the most current back-ups and the data that could be restored was one year old. Staff worked diligently to reenter any lost data.”

Library Board Meeting – Annotated Agenda

Monday, Sep 9, 2019, 6:00 pm

Notes prepared by Library Director Perry Stokes

Unfortunately, that episode wasn't the end of the matter for DCPL. A return of the malware was reported in July 2019.

BCLD defensive strategies include cyber education for staff through the SDAO webinar module, training on the importance of strong passwords, district-wide implementation of a password manager utility, and regular, secure backup routines.

VII. REPORTS

a. Director

Stokes

Attachments:

- VII.a.i. Publishers Weekly – The Week in Libraries (8.16.19, 8.23.19, 9.6.19)

Administration

None.

Friends & Foundation

The Friends are scheduled to meet on Tuesday 9/17/19.

No report from the Foundation.

Facilities & vehicles

The bookmobile is once again out-of-service due to persistent engine overheating. Troubleshooting seems to be repair by process of elimination. No word yet on the next suspect component.

Ed is arranging for ADA compliant hand railings to be installed at the Halfway branch. Expansion of the concrete landing at the meeting room entrance is a pre-requisite.

He is also preparing to begin replacement of the wood siding on the southeast corner of the Baker building (facing the staff parking area), which has deteriorated due to exposure and insects.

New "street-front" signage has been procured for Haines, Halfway, Richland, and Huntington branches. Ed is working on installation at each site. Repair and repainting of some of the posts is needed prior to attachment of the signs.

Professional carpet cleaning for the Baker branch is being scheduled for this month.

Ed has recommended removal of the large elm tree at the Northwest corner of the Baker branch. A significant amount of debris drops onto the roof, potentially puncturing the membrane, and regularly clogs the drainage spouts. Roots from the tree have caused heaving of the sidewalk approaches from the street and parking lot. He is coordinating with the Baker City Tree Board to obtain prior authorization before removal.

As mentioned in the public comment segment, I met with a local parent regarding disability access challenges experienced by her family. The parent had two primary concerns:

Library Board Meeting – Annotated Agenda

Monday, Sep 9, 2019, 6:00 pm

Notes prepared by Library Director Perry Stokes

- a. North parking lot: unauthorized parking encroachment into the designated ADA parking space hinders unloading/loading.
- b. Library-Park footbridge: debris from bridge deterioration and roughness of patchwork to the asphalt hinders wheelchair mobility.

I have directed Ed to restripe the ADA parking spot and procure new/additional signage to better designate the entire width of the area as ADA-use only. Ed is also looking into adding a second ADA parking spot on the other side of the evergreen tree there.

The footbridge is City property so we are urging their Public Works department to address the deterioration issues and evaluate overall safety. I have requested the bridge be included on the next version of the Parks & Recreation Strategic Plan, which is currently being crafted. Ed has recommended an overlay of asphalt to the bridge pathway pending a more comprehensive remodel/replacement. Until the structural integrity is evaluated, however, they will avoid adding more weight from asphalt and heavy equipment in its application.

Grants & Gifts

Donor Acknowledgment plaques have been delivered. Mounting in various areas are pending Facilities staff availability.

Marketing

Our TV guide ads for the next 9 weeks will be focused on promotion of Tutor.com for student homework help.

Personnel

We are currently experiencing a short staffing crisis due to a buildup of staff absences and resignations for personal and medical reasons. The Managing Librarian - Circulation & Operations Manager position has been revised and reposted as Library Associate I – Circulations & Operations Supervisor. We are also seeking to hire two substitute desk clerks (Library Assistant I), at least one of which may evolve into a regular position.

Our annual All-Staff Training event is scheduled for Oct 14 2019. As usual, the library will be closed to the public due to the Indigenous People's Day holiday. Staff receive the day after Thanksgiving as a holiday in-lieu of working on this occasion.

Programs & services

We recently responded to an inquiry from University of Oregon staff about our newspaper collection. They are interested in microfilming Record Courier issues from 2015-2016. I let them know we do have those issues and would be happy to provide them for that preservation project.

Safety & Security

Given the discovery this past year of discarded syringes on library grounds along the Leo Adler Pathway, we are updating Bloodborne Pathogen (BBP) kits at each branch and will be providing FDA-cleared sharps and medical waste disposal containers. Many thanks to Christine and Ed for working on this project.

Library Board Meeting – Annotated Agenda

Monday, Sep 9, 2019, 6:00 pm

Notes prepared by Library Director Perry Stokes

Technology

I am working with Jim on evaluation of new software to replace our Book a Room system. We have been using WordPress-based freeware for a year and it has been an effective tool to provide patrons and for staff to have better oversight of the booking requests.

Other

To keep the board informed of trending topics and events in the library profession, I aim to include The Week in Libraries articles from Publishers Weekly published since the prior board meeting. I recommend the board review these articles as part of meeting preparation and note any questions they inspire. This will serve as both board training and catalyst to discuss topics we already address or may need to address.

b. Finance

Hawes

Report documents to be distributed at the meeting.

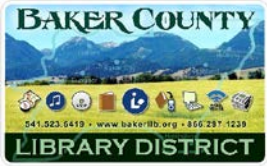
VIII. Next meeting: Oct 21, 2019

President-elect

- Future agenda items
 - Policy review/revision
 - Discussion of pro-rated benefits for part-time employees
 - Fee schedule
 - Library Card Eligibility
 - Social Software
 - Staff Use of Collection Materials
 - Digital Archive Copyright Statement / Rights Statements for digital cultural heritage object
 - Board Training: Discussion of ALA State of America's Libraries 2018 report

IX. ADJOURNMENT

President-elect



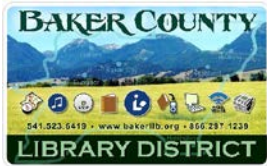
Baker County Library District

Board of Directors

Regular Meeting Minutes

Aug 12, 2019

Call To Order	The meeting was held in the Archive Meeting Room. Gary Dielman, President called the meeting to order at 6:10pm. Present at the meeting were Directors Gary Dielman , Frances Vaughan , and Betty Palmer , Directors. Also present were Perry Stokes , Library Director and Christine Hawes , Business Manager. Beth Bigelow was also present by invitation for an agenda item.
Consent Agenda	Dielman asked for any changes to the consent agenda which includes the agenda for tonight and minutes from the previous regular meeting. Stokes had an addition to New Business – County Clerk Forms. With no other changes, Palmer made a motion to approve the consent agenda; Vaughan seconded; motion passed (3 yea) .
Conflicts or Potential Conflicts of Interest	Dielman asked for any potential conflicts of interest. There were none.
Open Forum for general public	Dielman noted there were no members of the public present. Stokes had no correspondence to share but added that he did have one complaint about odors in the public restrooms which he will address in his Director Report.
OLD BUSINESS: Appointment to fill board vacancy	<p>Stokes introduced guest Beth Bigelow. She was one of the nominees to fill the board vacancy. If appointed, she is willing to serve out the remainder of Della Steele’s board term through 6/30/2021. Stokes asked if there were any questions for Beth about her background or credentials. Dielman asked Beth about her past interaction with the Haines Library. Beth described her background in teaching and school administration after moving to Baker City in 1978. She said she had been a teacher for many years and then served as the principal of Haines Elementary. She recalled her experience with taking kids to the library as teacher and her active library use as grandparent.</p> <p>Palmer said that she appreciates Bigelow’s ties to the community of Haines and feels it will be beneficial to the board. Dielman had one more question about Bigelow’s experience at North Baker School. Beth had been an administrator for five years at the Web Academy. There was some discussion on local grade schools. With no further questions, Vaughan made a motion that we appoint Beth Bigelow to fill the board vacancy; Palmer seconded; motion passed (3 yea). Dielman told Beth that she was now official and may vote during the rest of the meeting.</p>
NEW BUSINESS: County Clerk Oath of Office Forms	Stokes shared county provided Oath of Office forms to newly elected board members, Gary Dielman and Frances Vaughan. He also had an in-house Oath of Office form for Beth Bigelow to read and sign after having accepted the appointment to the board. Stokes will file the signed documents with library records.
SDIS Risk Management visit report	Stokes said that as part of Special Districts Insurance risk management program, an SDIS Agent, Phil Wentz conducted a property safety review of our district main branch



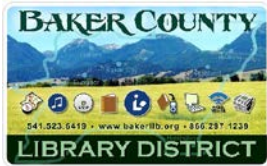
Baker County Library District

Board of Directors

Regular Meeting Minutes

Aug 12, 2019

	<p>on April 16, 2019. The results of that visit are included in the packet. The letter summarizes the findings shown on the Risk Management Visit report that follows.</p> <p>There were two severe issues:</p> <ol style="list-style-type: none"> 1. The roof which we are aware of and have a plan in place, and 2. The wood siding on the south side of the large meeting room. <p>The siding is a high priority due to a carpenter ants infestation and the poor condition of the siding. It is on the list for Ed to replace the wood siding this fall. He will be replacing it with a Hardy Plank product.</p> <p>There were two moderate issues cited:</p> <ol style="list-style-type: none"> 1. Wrinkles in the carpet outside the main public bathrooms. Ed has addressed the issue, cut the carpet to make repairs and glued it back down. The carpet will be one of next large items that need to be addressed, and 2. The riverside wooden boardwalk deck is deteriorating. This project is also on Ed's list of priorities for fall. Ed reports the support structure is sound. The decking will likely be replaced with Trex Decking. <p>The minor items cited were discussed briefly.</p> <p>Regarding public complaints of odors in the bathroom, Stokes stated that only one of the eight bathrooms seems to have sufficient ventilation. Ed has looked at installing ventilation fans, but those will have installation challenges. Palmer said that she appreciates our Facility Maintenance staff, Ed Adamson and his ability to address so many things. She also appreciated the letter he wrote to the board addressing the site visit assessment concerns.</p> <p>Stokes said that more facility maintenance issues are anticipated as the building ages. The district will accomplish projects as budget allows but may need to look at a bond sometime in the next 10 years for a comprehensive remodel. There was no further discussion.</p>
<p>Authorization of auditor engagement letter</p>	<p>Stokes described a meeting with CPA Jake Collier regarding the significant audit fee increase. Collier had explained that the firm Guyer & Assoc. has increased requirements and procedures on their side of the audit. They had not looked at their services pricing for some time. He emphasized that the bid is the highest they would bill and would be happy to bill it lower if it comes in lower.</p> <p>The board agreed with Stokes' suggestion that putting the audit contract up for competitive bid would help ensure that the district is not paying more than fair market value. There was discussion on the potential of filing an extension and having</p>



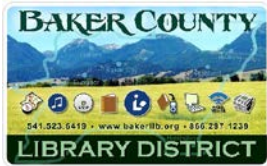
Baker County Library District

Board of Directors

Regular Meeting Minutes

Aug 12, 2019

	<p>the audit done next spring which would give the District time to do a formal bid process.</p> <p>Palmer voiced support for an RFP to see what happens. The board directed Stokes to put an RFP out with a deadline before the September regular meeting. It was acknowledged that the short time frame could be a hindrance to bids.</p> <p>Should no competitive bids be submitted, the board is willing to continue engagement with Guyer & Associates to keep the audit process and report on schedule.</p>
<p>REPORTS: Director Report</p>	<p>Stokes gave the Director’s report:</p> <p>Administration – The FY2019-2020 budget documents have been filed with both the County Assessor and Clerk as required by law.</p> <p>Friends & Foundation – The Friends Summer Book Sale grossed a little less than usual at about \$1,600. The reduced gross is possibly due to a reduction of prices on higher value items as a strategy to reduce excess surplus inventory. Un-sold items were either shipped to a book reseller that takes selected items, offered as free giveaways, or disposed of in the landfill. Foundation – no report.</p> <p>Vehicles – The bookmobile has resumed its regular schedule.</p> <p>Facility – Scotts Heating replaced filters in the HVAC units at the Baker, Richland, Halfway and Huntington branches as regular maintenance. The filters are high-priced; the maintenance invoice total was \$2,987. Ed made repairs to the floor to fix a hazard area outside the main public restrooms. When he pulled back the carpet, he found tiles on the subfloor had broken and heaved up, causing a tripping hazard. That was repaired, sealed and the carpet glued back down. Carpet replacement has been put on a long term strategic plan. It may need to be done in stages over time. Ed also replaced a valve in the children’s bathroom.</p> <p>Grants – Stokes has authorized Children’s Specialist, Missy Grammon, to apply for Leo Adler funds to remodel the Storytime and children’s lab rooms. There is a need to create a youth/tween lounge similar to the teen room to allow that age group to have an informal gathering place.</p> <p>Marketing – Stokes has invested in one year of advertisements in the Weekly TV Guide published by the Baker City Herald. The library’s ad space is at the bottom left on page 2. He aims to feature the many premium services and opportunities available at the library.</p>



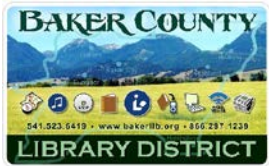
Baker County Library District

Board of Directors

Regular Meeting Minutes

Aug 12, 2019

	<p>Programs & Services – Summer Academy school administrators expressed their gratitude for Missy and the library’s partnership in that program. Palmer described the Summer Academy benefits and growth seen in reading skills and number of participants. The goal is to keep kids’ skills from backsliding over the summer and build their reading enjoyment and ability.</p> <p>Personnel – One of the district’s Managing Librarians, Nola Huey resigned as of 7/31/2019 due to family needs. The position will be filled by internal staff. The position’s many responsibilities are being evaluated; some duties may be re-assigned. IT Systems Manager, Jim White, has retired and been re-hired as retiree, now working part-time as of August 1. The IT Department has also lost IT Assistant, Bryan Ames, who is leaving for college at the end of August. Stokes is working with White to develop a succession plan for network sustainability in case of emergency and Jim is unable to work for an extended period of time. Jim has vastly increased network capacity and maintenance efficiency over the years. Stokes aims to develop an RFP for emergency IT support services.</p> <p>Stokes plans to contract with a materials recovery service, aka collections agency this year. The district occasionally utilizes local law enforcement to seek restitution in extreme cases, but this tactic is not very effective on people who move out of the area.</p> <p>Stokes described the evolution of the library’s annual staff party events over time. After participation in the Bowlstice dwindled, staff have tried new things. The murder mystery event last year was a great success and well attended. This year Nola came up with the idea of an Amazing Race theme for a team building event. Board members are invited to participate on Saturday 9/21. An RSVP will be sent soon via Google Forms.</p> <p>Safety & Security – Stokes has ordered new, larger, signage to improve public notice about Security System presence and No Smoking/Vaping.</p>
<p>Finance Report</p>	<p>Hawes handed out check packets for signatures. The financial report had already been added to the board report packets.</p> <p>The General Fund received tax turnovers of \$4,144.20 on August 1, 2019. The turnovers were all prior taxes. Personnel Services is on target with the budget in total. Under Materials & Services, looking at the Books budget, large expenditures included Ingram book order of \$6,554.83, NewsBank \$1,958.00 for the Baker City Herald online subscription and Tutor.com \$1,500.00 to continue the online tutoring subscription. Stokes added that the Tutor service expanded the hours. He will aggressively promote it at the schools in hope it will get more use. Hawes stated that</p>



Baker County Library District
 Board of Directors
Regular Meeting Minutes
 Aug 12, 2019

	<p>another notable check is the District Visa of \$4,838.21 the details are attached to the check for review. In Buildings & Grounds Maintenance, Busy Bee Carpet Cleaning \$1,040.50 for carpet cleaning at 2 branches, Jack Rudd Plumbing \$250.00 for a plumbing consulting and service call, and Scott's Heating \$2,986.88 for HVAC maintenance mentioned earlier. The bookmobile repairs this time were \$1,066.00 paid to Mike Bork Auto Repair.</p> <p>Other Funds received Amazon book sales revenue of \$517.50. No other income. This fund wrote a check to Visa for shipping the books sold of \$70.74.</p> <p>Sage Fund had no income. This fund wrote a check to Orbis Cascade for the last invoice for services to BMCC \$6,176.37 and a new courier service in Pendleton, Banks Courier \$1,315.00. It also sent an electronic payment to Jon Georg for his monthly system maintenance contract payment of \$5,100.00. Current cash is low at \$130,373.43. Sage sends out membership billings in October.</p> <p>Hawes asked if there were any questions about the financial report. There were none.</p> <p>The Directors signed the checks and initialed the check list approving the bills paid since the last meeting.</p> <p>Discussion ensued on the Summer Academy topic. Stokes described the budget and library operations for the new board member.</p>
<p>Next Meeting Date</p>	<p>The next regular Board meeting will be September 9, 2019.</p>
<p>Adjourn</p>	<p>The meeting was adjourned at 7:13 pm.</p> <p>Respectfully submitted,</p> <p>Perry Stokes, Secretary to the Board</p> <p>PS/ch</p>

BILL TO:

Baker Co Library Dist
Accounts Payable
2400 Resort St
Baker City OR 97814

Rivistas Subscription
Services
2824 Columbia Ave
Wilmington, NC 28403
Service@Rivistas.com
1-800-277-5750

Ship To	Quote ID	Rate	Total
Baker Co Public Library 2400 Resort St Baker City OR 97814	9273	18.00 %	\$5,250.63
Baker Co Public Library 2400 Resort St Baker City OR 97814	9277	18.00 %	\$16.40
Haines Branch Library 818 Cole St Haines OR 97833	9280	18.00 %	\$0.00
Halfway Branch Library PO Box 922 Halfway OR 97834	9275	18.00 %	\$143.42
Huntington Branch Lib PO Box 130 Huntington OR 97907	9276	18.00 %	\$129.72
Richland Branch Library 42008 Moody St Richland OR 97870	9278	18.00 %	\$148.63
Richland Branch Library 42008 Moody St Richland OR 97870	9274	18.00 %	\$19.68

Ship To	Quote ID	Rate	Total
Sumpter Branch Library PO Box 67 Sumpter OR 97877	9279	18.00 %	\$198.57

Total

Total Subs	1656
Total List	7,130.13
Discounted Total	5,907.05

BILL TO:
Baker Co Library Dist
Accounts Payable
2400 Resort St
Baker City OR 97814

Rivistas Subscription
Services
2824 Columbia Ave
Wilmington, NC 28403
Service@Rivistas.com
1-800-277-5750

Ship To	Quote ID	Rate	Total
Baker Co Public Library 2400 Resort St Baker City OR 97814	9277	18.00 %	\$16.40
Baker Co Public Library 2400 Resort St Baker City OR 97814	9281	0.00 %	\$3,709.16
Baker Co Public Library 2400 Resort St Baker City OR 97814	9273	18.00 %	\$5,250.63
Haines Branch Library 818 Cole St Haines OR 97833	9280	18.00 %	\$0.00
Halfway Branch Library PO Box 922 Halfway OR 97834	9275	18.00 %	\$143.42
Huntington Branch Lib PO Box 130 Huntington OR 97907	9276	18.00 %	\$129.72
Richland Branch Library 42008 Moody St Richland OR 97870	9278	18.00 %	\$148.63

Ship To	Quote ID	Rate	Total
Richland Branch Library 42008 Moody St Richland OR 97870	9274	18.00 %	\$19.68
Sumpter Branch Library PO Box 67 Sumpter OR 97877	9282	0.00 %	\$238.60
Sumpter Branch Library PO Box 67 Sumpter OR 97877	9279	18.00 %	\$198.57

Total

Total Subs	2109
Total List	11,077.89
Discounted Total	9,854.81

Ransomware attacks on the rise — and small towns are in the crosshairs



Preventing ransomware attacks ahead of 2020 election

- There were more than 70 ransomware attacks in the first half of 2019 — and more than 50 of them targeted cities.
- "We are definitely seeing more, and we see them because attackers see that they're successful," said one cybersecurity professional.
- The rise in attacks has led to a rise in cyber insurance products that are more profitable than many other insurance types.

An upstate New York school district delayed the start of the school year on Wednesday after a ransomware attack hampered its operations. The Orange County school district joins an unhappy parade of municipalities that have fallen victim to hackers.

Two Long Island school districts were hit by ransomware earlier this summer. Last month, nearly two dozen cities in Texas fell victim to what has been called a "coordinated" attack.

In the first half of the year, more than 50 cities or towns were the victims of ransomware attacks this year, according to a recent report from Barracuda, a cybersecurity firm. Indeed, two-thirds of more than 70 ransomware attacks tracked in the U.S. focused on local or state governments, according to the report.

"Local, county, and state governments have all been targets, including schools, libraries, courts, and other entities," it found.

22 local Texas governments tackle coordinated ransomware attack

Smaller locations are at particular risk. Nearly half of the municipalities attacked had between 15,000 and 50,000 residents. A quarter had fewer than 15,000 residents, Barracuda said, noting that "smaller towns are often more vulnerable because they lack the technology or resources to protect against ransomware attacks."

The average ransom payout in the second quarter of this year was \$36,295, according to a report by [Coveware](#). That's nearly triple the average payment in the prior quarter. In the third quarter of 2018, when Coveware first started tracking payments, the average was \$5,973.

Ransomware attacks have been on the rise in recent years because of how profitable they can be for attackers — and smaller cities are an attractive target. In addition to lacking resources, cities are

often dealing with taxpayer money and so may elect to pay a ransom rather than try to recover their data in another way, said Wendi Whitmore, vice president of X-Force Threat Intelligence at IBM Security.

"We are definitely seeing more, and we see them because attackers see that they're successful," said Whitmore.

"A lot of times we have clients think it's a one-time cost," she added. But "If you pay the ransom, you still have to fix the [security] problem so the same thing doesn't happen tomorrow."

Not all cities opt for a quick fix. Barracuda found that of the 50 municipal attacks over six months, only three cities chose to pay the ransom. Many others are instead fighting it out, with mixed levels of success. Baltimore, which was attacked in May, refused to pay a \$76,000 ransom; it has to date spent more than \$5 million recovering the data lost in the attack, ProPublica [reported](#).

U.S. officials reportedly designing program to prevent ransomware attacks in 2020

The increase in attacks is driving a rise in cyber insurance — a rare new area of growth in the insurance industry. Cyber policies are more profitable for insurance companies than policies overall, according to a 2018 report from Aon, and last year, insurers collected \$2 billion on premium on these policies. The number of cyber insurers is also rising, increasing 54% over four years.

But the quick growth of cyber insurance could itself be a factor driving increased attacks, ProPublica found. Insurers have encouraged hacked clients to pay the ransom rather than fight the attackers, on the grounds that it would save time and money, ProPublica reported. And there is some evidence that hackers are specifically going after companies they know have cyber insurance, presumably because they're more likely to pay up.

Whitmore recommends that organizations keep a backup of essential files that is disconnected from their main network so that, in case of an attack, hackers won't be able to seize all the files. She also suggested organizations rehearse their plan in case of a cyber attack, much like in a fire drill.

"You may not be able to use company email to get hold of everyone, so do we have the ability, in advance, to get a hold of everyone? It could be a WhatsApp group or Gmail," Whitmore advised.

Ransomware Hackers Target Government Offices, Libraries

by [Matt Enis](#)

Apr 04, 2017 | Filed in [News](#)

Ransomware attacks on government offices, civic agencies, and schools are on the rise, and include a January 19 attack on the St. Louis Public Library (SLPL). Ransomware is a form of malware that encrypts files on a computer or network. The individual or organization responsible for the attack then demands a ransom, generally paid to an anonymous Bitcoin account, to provide a key necessary to decrypt the files.



An average of more than 4,000 attacks per day occurred in 2016, representing a 300 percent increase compared to 2015, according to estimates in "[How to Protect Your Networks from Ransomware](#)," an interagency technical guidance document issued by the U.S. Justice Department and U.S. security agencies. In September 2016, security ratings provider [BitSight](#) released a [report](#) from an analysis of nearly 20,000 companies and institutions, noting that the rate of ransomware attacks increased significantly for every industry examined during the 12 months prior, with the education sector facing the highest rate of attacks, and government organizations facing the second-highest.

In addition to SLPL, other attacks so far in 2017 include [Licking County, OH](#); the library server system for [Hardin County Schools, TN](#); [Bingham County, ID](#); and the network of the [Pennsylvania Senate Democratic Caucus](#).

SLPL's attack came to a relatively positive conclusion. The library had backups for the files that were encrypted and refused to pay the ransom, according to an open letter to the community by SLPL executive director Waller McGuire. SLPL's website, catalog, and downloadable materials were unaffected. After regaining control of the affected portions of the

network, SLPL prioritized patron services. The library's IT staff had the checkout system operational by January 20, the day after the attack, and had restored hundreds of public computers by January 21.

In the January 30 open letter to patrons, McGuire noted that "all St. Louis Public Library technology used by patrons has been restored to service.... Free printing for patrons was one of the last public services to be restored last week." For most patrons, the library seemed back to normal within a day or two of the attack, McGuire said, even as work continued behind the scenes to complete the restoration of the network. "There were many 48-hour days and much exemplary work trying to quickly give the library back to our patrons," McGuire wrote. "Staff here believe deeply in the mission of the library and I'm proud of them. Many of you have expressed concern and support, and we thank you for it."

WHAT TO DO

As the SLPL's case illustrates, regularly scheduled backups are the best insurance against ransomware attacks. Individual users should regularly back up important files to a portable hard drive or flash drive that is not regularly connected to their system and/or a secure cloud-based backup system (not Dropbox). Restoring those backups and recovering from an attack will cost an organization time and money, but the Federal Bureau of Investigation (FBI) and other security agencies note that there is no guarantee that an attacker will provide the decryption key to unlock an encrypted system if a ransom is paid. Some attackers, once paid, immediately request additional money. Others provide the key, but then target the organization again. Others simply disappear without providing the key. And, "paying a ransom emboldens the adversary to target other victims for profit, and could provide incentive for other criminals to engage in similar illicit activities for financial gain," according to the FBI's September 2016 [public service announcement regarding ransomware](#). However, the agency does add that "it recognizes executives, when faced with inoperability issues, will evaluate all options to protect their shareholders, employees, and customers."

In a fall 2016 attack on the government offices of Madison County, IN, affecting 600 workstations and 75 servers, the county's cyber-insurance provider Travelers resolved the attack by paying the ransom, minus a deductible paid by the county, according the *Herald-Bulletin*. The amount

was not disclosed, but the county is reported to have spent nearly \$200,000 since the attack for off-site data storage, improved firewall protection, and a backup system for its courts.

The FBI is urging victims of ransomware attacks to report these crimes—regardless of the outcome—to a local FBI office and the Internet Crime Complaint Center at [IC3.gov](https://www.ic3.gov) to help the agency understand the threat, monitor the spread of ransomware variants, justify the dedication of department resources to this issue, and ultimately combat the individuals and organizations responsible for creating the malware and launching attacks. Requested information includes: the date of infection, the ransomware variant, the victim or company information (industry type, business size, etc.), how the infection occurred, the requested ransom amount, the attacker's bitcoin wallet address, the ransom amount paid (if any), overall losses caused by the attack including any ransom amount paid, and a victim impact statement.

Separately, the MalwareHunterTeam, a group of security experts led by ransomware researcher Michael Gillespie, hosts [id-ransomware](https://www.id-ransomware.com), a site that enables victims to upload a ransom note or an encrypted file to identify which Ransomware variant—from a group of almost 350 known types—is affecting their computer or network, and in some cases, whether a decryption key may have been published for that variant. With this method, the team also regularly discovers new variants and reports them via outlets such as the technical support and news site [bleepingcomputer.com](https://www.bleepingcomputer.com), which hosts FAQs, articles, and help guides on ransomware and other malware. [NoMoreRansom.org](https://www.nomore ransom.org), an initiative of The European Cybercrime Centre (Europol EC3), the National High Tech Crime Unit of the Netherlands' police, Intel Security, and Kaspersky Lab, also hosts more than three dozen [decryption tools](#) for common ransomware variants that have been cracked by security experts.

An affected library may also want to follow the lead of SLPL, and issue a statement to the local media and to patrons, reassuring the public that their data has not been compromised. Unlike many other forms of hacking directed at organizations, ransomware attacks to this point generally have not involved the theft of data or personal information—only encryption and, with several variants, the threat of indiscriminate file destruction if a ransom is not paid within a specific timeframe. In SLPL's case, patron information was stored elsewhere and was completely unaffected by the attack, McGuire explained in the library's statement.

“I want to repeat two assurances to the community,” McGuire wrote. “First, our main concern was investigating whether any personal information had been exposed by this attack. Because of the way our system is designed, patron information, such as addresses and phone numbers, is held in a remote location and kept secure. It was not accessed. If you have used a credit card at the library, that information has been recorded only on secure, encrypted lines by banks. It was not accessed.” He continued: “Second, the St. Louis Public Library never paid any ransom. Staff brought the demand to me within moments of discovering it, and we were on the phone with the FBI moments later. Although I understand that the decision to pay can be complex for many institutions and companies, SLPL never considered it.”

OUNCE OF PREVENTION

McGuire notes that SLPL’s IT staff is well aware that its network is constantly probed for vulnerabilities. In this case the point of entry was found to be a four-year old voicemail server with an unpatched security vulnerability. Even the most vigilant staff won’t be able to fix problems that vendors don’t know about, haven’t warned their customers about, or simply haven’t fixed. Similarly, an article published last week by *Government Technology* describes a recent ransomware attack on the government of Livingston County, MI, that was triggered by malvertising on a trusted local news website. But much of the usual advice about avoiding viruses and malware applies here as well.

In “How to Protect Your Networks from Ransomware,” government agencies are advised to create and implement a training program to make employees and individuals more aware of these threats and how to prevent them. As the FBI and nomoreransom.org advise, keep all software up to date and apply patches when available. Don’t open unsolicited email attachments from unfamiliar people or companies. More broadly, recognize that even the accounts of friends and associates may be compromised, and never open any attachments that seem suspicious, even if the source is usually trusted.

The U.S. Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security, has published a guide to “[Avoiding Social Engineering and Phishing Attacks](#)” with more granular suggestions. And, in a May, 2016 *WIRED* article “[4 Ways to Protect Against the Very Real Threat of Ransomware](#),” Stu Sjouwerman, the CEO of computer

security training company KnowBe4, suggests gamifying awareness training by sending employees simulated phishing attacks to help them understand what these threats look like. Windows users should consider disabling the “[hide extensions for known file types](#)” option in Windows settings to make it easier to spot suspicious, executable files that have been disguised as something else, with names like filename.doc.exe or filename.pdf.vbs.

“How to Protect Your Networks from Ransomware” also suggests that IT departments set their systems to filter out executable files from incoming and outgoing emails, to disable macro scripts from any office files transmitted via email, and to assign administrator privileges to individual employees only when absolutely needed. Individual users could consider disabling remote desktop connection and remote assistance features as well, although this won’t be practical in many workplace environments in which IT departments use these features to help staff and troubleshoot workstations.

NoMoreRansom.org encourages individuals to use antivirus software with heuristic scanning/analysis features and be sure to leave those features activated, enabling the software to detect newer, undiscovered malware variants based on suspicious behavior by a program. And employees should know to immediately power off a network-connected workstation or device if they believe it has been infected with ransomware, and then notify IT.

Crime	FBI	ransomware
-------	-----	------------

RELATED →

NEWS

Essential Techniques For Life Science Research

When Ransomware Attacks

How three libraries handled cyberextortion

By [Greg Landgraf](#) | June 1, 2018



On the morning of January 29, a library technician at

Spartanburg County (S.C.) Public Library (SCPL) encountered a notice on the library website announcing that its computers had been encrypted with ransomware. The library immediately shut down all computer-related services to quarantine the malware.

County Librarian Todd Stephens says that he and his colleagues suspect the attack came through an infected email message opened by a staff member, though the exact mechanism is uncertain. The anonymous attacker demanded 3.6 to 3.8 bitcoins in payment—then valued at about \$36,000.

Ransomware, a form of computer malware that encrypts a victim's data to extort payment, is one of the fastest-growing computer security threats. In 2017, such attacks cost businesses, individuals, and other organizations an estimated \$5 billion, up from \$325

million in 2015, according to research firm [Cybersecurity Ventures](#).

And while libraries haven't been singled out as targets, libraries like SCPL can attest to the logistical headaches that can follow. Much of the library's day-to-day functioning was seriously affected. SCPL took down its website, public catalog, digital collections, and intranet. Circulation was interrupted, although staff began manually checking out materials with handwritten barcode numbers within a couple of days.

SCPL Coordinator of Systems Chris McSwain says the library had 23 servers that were encrypted to some extent, and many of its client computers were affected as well. The attackers did not capture any sensitive user data: Credit card information used to pay fines is kept by a third-party vendor and wasn't encrypted, and the library doesn't keep other sensitive data like Social Security or driver's license numbers.

The library refused to pay the ransom. "You have no guarantee that what you're getting back is clean data or hasn't been replicated," Stephens explains.

Trouble elsewhere

Brownsburg (Ind.) Public Library was similarly resourceful when it suffered a ransomware attack on June 26. Director Denise Robinson was attending the American Library Association's Annual Conference when she received a call from staff members who couldn't log in to their computers. "We think that when the server rebooted to do a Windows update, our SQL database got infected," Robinson says. The SQL database operates the library's integrated system, so patrons couldn't search the catalog or check books out.

As a stop-gap solution, "we did a lot of creative searching to find books, like using Indianapolis Public Library's catalog to determine where a requested book would likely be," and manually circulating books, Robinson says.



After losing computer access during a ransomware attack, Brownsburg (Ind.) Public Library processed book checkouts and returns manually.

After attempting to restore the encrypted systems, the library ultimately paid the attackers' ransom demands—half a bitcoin, worth about \$1,500 at the time. Robinson says the library's decision to pay the attackers came about because its most recent full backup was three months old. Fortunately, the library received the unlock code only a few hours after it made the payment. Systems were back online within three weeks.

At Hardin County (Tenn.) Schools, which suffered an attack on its library computer network over the 2016–2017 winter break, hackers demanded 1.5 bitcoins—then worth \$1,341—with an increase to \$1,788 if the demand wasn't immediately met. “After much research, it was decided that we would not pay the ransom,” says Technology Coordinator Levin Edwards. Instead, the school was able to decrypt some backup files.

That success was only partial, however, as the “backup files were two years old. The librarians had to do their best to update the missing information,” Edwards says. As a result of the attack, students were unable to check out books from the school library for about four weeks.

Lessons learned

It's likely not possible to prevent ransomware incidents completely. “The attacks are sophisticated and will continue to morph,” Stephens observes.

There are, however, ways to defeat some attacks or mitigate their impact. “Have backups and test them fully—not just that you can restore files,” McSwain advises. Keeping a virtual backup also works, he adds.

SCPL is strengthening its password policies, limiting the use of third-party apps by staff, and auditing its security systems, but it's also addressing the human side of the equation. “We're working with staff to be very thoughtful about the emails that come in,” Stephens says. The library intentionally sent a phishing email to staff to learn how they interact with potentially dangerous messages.

In Brownsburg, Robinson says that the library now has enhanced the security precautions in place and that “we do backups every night now” with an offsite backup every 30 days. The library also installed Cylance, an antivirus package that identifies and prevents patterns of activity related to malware.

Robinson says patrons have been understanding and sympathetic, thanks in part to the library's transparency about the situation. "Sharing as much information as we could really put people at ease," she says. In particular, the library confirmed that the only personal data it retained were patron names, phone numbers, and addresses—no credit card or Social Security information. And, while the manual checkouts could have provided an opening for unscrupulous patrons to steal library materials, an end-of-year inventory found fewer than 2,000 items unaccounted for—some of which had been weeded anyhow—out of a collection of 100,000.

SCPL also put a priority on communications. The day of the attack, the library posted signs about the shutdown of computers while it assessed the situation. The next day, when it was clear what was happening, the library notified trustees, the county council, media outlets, and its social media outlets. Stephens also used the library's emergency text notification to provide updates to staff at least once a day for the next week and a half.

Library administration and IT staff also need to be in regular communication, Stephens advises. He and McSwain met three times a day for three weeks during the recovery. One additional piece of advice he offers for the long days that IT staff will face bringing systems back online: "Make sure you buy their lunch."

GREG LANDGRAF is web content specialist at Greene County (Ohio) Public Library and a regular contributor to *American Libraries*.

Libraries, Beware: Ransomware

Posted on [May 23, 2019](#) by [Henry Stokes](#)

Regardless of whether you are urban, suburban, or rural, or serve smaller or larger populations, if you work at a library, school, or university, you are a target for ransomware attacks.

Not sure what ransomware is?

You're not alone. A recent study showed that **64% of working adults** don't know either. And that's a problem because ransomware is on the rise and getting more and more sophisticated, targeting businesses of all sizes and in all parts of the country. Libraries are no exception.

Ransomware is a type of malware (malicious software) that takes over your computer system until a sum of money is paid. Usually this means that your files become encrypted and only the attackers know the key. When a targeted organization's servers are infected, many of the most important services are shut down and held hostage. For a library, this may result in no access to the public computers or WiFi, to the library's website and ILS to borrow materials, as well as to other digital services that patrons have come to rely upon everyday.

Are people actually paying the money?

Turns out that 30-60% are indeed paying the ransom, but reports reveal the sad truth that 20% of them never get their data back. In these instances, the criminals get paid but don't end up following through with providing the key. Not only that, but reinfection rates are skyrocketing with even the backups (meant to help safeguard against attacks) getting hit too.

The main defense of antivirus software is often not enough. 94% of victims had the antivirus software running when hit by ransomware. This is because traditional anti-virus software uses blacklisting – a technique to locate malware files and deny them access or ability to install or be run. But this doesn't work as well as it used to. Ransomware is morphing way too fast with 99% of it lasting only 58 seconds, and even then, it's only seen once. As a result, the blacklisting antivirus software can't keep up. So what if it found one and kept it at bay? So many more are popping up, like overwhelming armies of undead, trying to breach the walls. An even more sobering thought is that ransomware is getting easier and easier for the criminals to do; it's fully automated now with cheap kits and how-to guides readily available on the Dark Web.

The [State of K-12 Cybersecurity Year in Review](#), a report released a few months back, shows the extent of the problem in school districts across the U.S.

How does a library get attacked by ransomware?

Phishing ([read my blog post for more info](#)) is usually the culprit, or an infected email message opened by a staff member. The real cause is what's called the "Human Factor". The people themselves are the weakest link in cybersecurity.

How do you prevent it?

Here are five ways to defend against the infection and impact of cryptoviral extortion:

1. Start with staff education. Make sure everyone working at the library has training on basic online security practices such as how to avoid phishing attempts. Need curriculum? There are great resources from the [Digital Patron Privacy Project](#) and the [Library Freedom Institute](#).
2. Strengthen your password policies. Passwords are the main line of defense we use to secure our data. If passwords are weak, one is really opening oneself up to malware attacks. See how strong a password is from a [password check site](#).

3. Use multi-factor authorization (MFA) whenever it is available. This is the next level of protection beyond the single password. Google accounts, for example, encourage [2-step verification](#) where users must provide both their password, plus an additional code sent immediately to their phone via text or voice call. It's recommended to use MFA on all administrative accounts.
4. Keep software, including the antivirus and OS (operating system), patched and up to date.
5. Have backups and *test them fully*, not just that the files are restored. You may consider doing backups every night, with an offsite backup every 30 days. This way, if an attack does happen, you are prepared.

Help! My library was attacked with ransomware! Now what?

Well, first off, it may not be advisable or worth it to pay. As [County Librarian Todd Stephens at Spartanburg County \(S.C.\) Public Library said to ALA](#) after his library was attacked: "You have no guarantee that what you're getting back is clean data or hasn't been replicated."

Here are a few tips to keep in mind if the library is attacked and you want to handle it without paying:

- Find out what was affected and encrypted. Cloud-based, third party vendors (such as for websites, ILS software) may have data protected from the attackers' hijacking. If you find that you can still navigate the system and access files, the ransomware notice may just be a fake attempt to scare you and you can ignore the ransom note. If it is indeed encrypting ransomware, ensure that credit card information stored for patrons to pay fines or other sensitive data like Social Security or driver's license numbers weren't compromised.
- To restore your data, there may be a logistical headache in your future. You may have to research decryptors that can remove your particular strand of malware. You may also have to go analog for a bit while you address the problem and begin checking out library materials the old-fashioned way, with paper and pen.
- Be sure to be transparent with patrons about the situation, confirming exactly what information was and wasn't affected. It will put them at ease and should even generate good will and sympathy towards the library. Also, use good communication. Place signs above the shut down computers, for example, and notify trustees, the county council, media outlets, etc.

Two weeks ago, Daviess County Public Library in Kentucky was a victim of ransomware. One can learn a lot from how they handled it. Check out this one-minute video they made for their patrons, thanking them for their patience. I think it does a great job of communicating the issue (in a fun, not overly-panicky way), as well as showing how much hard work is involved and how good-natured and dedicated the staff is. Well worth a watch!

Video from DCPL about their ransomware attack.

If you'd like to learn more about the Kentucky library attack, this [article](#) includes a description of exactly how much data was lost and how they handled the process of inventorying their entire collection. They were able to piece together quite a lot of their information because they were using vendors that had cloud storage. Their patron information was the hardest hit it seems:

"Because we work with other companies, our data is shared, that was not affected," she said. "We were able to go to them and say we need that info. We mostly lost the patron account information. Anyone that got a new account or updated their account since April 2018 will have to come back in so we can get them set up in the system. We have change of address forms with the basics. They will fill that out and we will have data entry people setting that up."

If you are at a Texas library and have more questions about phishing, passwords, multi-factor authorization, backups, ransomware, and digital patron privacy, contact [Henry Stokes at the Texas State Library](#), 512-463-6624. The Continuing Education & Consulting (CEC) team is available to provide in-person workshops on this topic as well.

Library still plagued by ransomware

By Jacob Mulliken Messenger-Inquirer Jul 18, 2019



Erin Waller, Daviess County Library Director

Maria Clark

The Cryptolocker ransomware that crippled the Daviess County Public Library in April is back and slowing various library services.

In actuality, it never left, said Erin Waller, library director, despite the efforts of the library's IT (information technology) staff.

Cryptolocker is a specific form of ransomware that focuses on a victim's data to extort payment with the threat of losing that data if the ransom isn't paid in full. Even then, there is no guarantee that the hackers behind the virus will actually come through with the key to free the data, she said.

"According to outside experts that we brought in to aid us this time around, once hackers get in, they hang around hoping to get another payoff," she said. "You think you have done everything to clean it out and start over, but they are hiding, waiting to pop up again when you are vulnerable to ask for more money. We are realizing that this malware is super-aggressive"

The library's current woes began on July 8 when Waller and her staff began to notice white screens popping up on customer self-service screens, she said.

"We were still gun-shy," she said. "At the time, we didn't know. We thought that it had something to do with the past attack or the work we are doing to strengthen our system. We just weren't sure. We shut things down really fast so it didn't keep growing. We didn't lose anything because we have great backups, then and now. We had some services that were down last week and we were finding strange files on staff computers, so we were taking each computer and running a scrubbing software."

On Monday, library staff felt that the situation was under control and that everything was back to form, until Wednesday, when it became apparent that April's virus was still alive and well, she said.

"This past Monday, we felt like everything was good," she said. "We were feeling confident and started turning things back on to get back to normalcy. Monday and Tuesday were good. Wednesday is when the white screens were back and we realized that it (the virus) is bigger than us and we needed to call in some experts."

One of the experts, Bill Uptmore, compared the virus to the classic arcade game Whac-A-Mole, Waller said.

"You knock it down and it pops back up elsewhere," she said. "This is a super aggressive malware and now that we know what is happening, we have a better idea of how to tackle these issues."

The library was initially attacked on April 28. Their files were encrypted and held ransom for six bitcoins, or \$30,947, which the library did not pay. Ultimately, the library was forced to close its doors May 7 through May 9 to address issues and have employees re-inventory its more than 300,000 items.

While they are hoping to avoid closing like they did in early May to re-inventory and address data issues, certain services are suspended so that Waller's staff and outside aid can address the virus, she said.

"There are no internet services in the building right now," she said. "People can't access the catalog or their accounts from home, but we can here and we are only allowing people to check out 15 items at a time. We are working really hard to improve every day, but it will take some serious recovery. I want to stress that no data was lost or compromised and no one's data is out there. We will follow the recommendations of our outside experts in terms of the extent of the problem and solutions. We will be here for people as much as we can. If we close, it is because we have to. That decision will not be done lightly."

Jacob Mulliken, 270-228-2837, jmulliken@messenger-inquirer.com

THE OWENSBORO TIMES

Ransomware attack hinders library for second time



by The Owensboro Times — Wednesday, July 17th, 2019 11:21 pm in Community, News



Photo by AP Imagery

Daviess County Public Library is offering patrons another unexpected amnesty on fines for overdue materials after a ransomware attack has limited access to some of the facility's computers for the second time in three months.

According to the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), ransomware is malicious software that prevents access to systems or data until a ransom fee is paid to the attacker. Once a network has

been infected with ransomware, the malicious software attempts to spread to storage drives and other accessible systems.

On Wednesday, DCPL issued a statement on social media responding to patrons who were concerned when they were not able to access their online account via the library's website.

"...Unfortunately, the malware attack we experienced in April was never fully resolved," the statement said. The statement also explained that although the recovery process will be lengthy, the library guarantees "no personal information was breached."

DCPL Director Erin Waller told the Owensboro Times, "this type of malware is encryption malware. They aren't interested in or even have access to [patron personal info]...they just want to ransom the encryption key."

CISA explains that if the attackers demands aren't met, data may simply remain unavailable or be deleted from the system. However, the agency warns against entities paying a ransom to attackers noting organizations have no certainty they will actually regain access to their data and could make themselves larger targets for future attacks.

When asked if DCPL had paid a ransom in the past or plans to pay the current ransom, Waller responded, "Absolutely not."

After reviewing references, the library has secured an expert to assist with the recovery process. According to the library's statement, the expert believes "a resolution is in sight."

CISA claims preventative measures through training and awareness programs are the most effective defense against ransomware. Waller says once the library gets past the ransomware attack there are plans to implement training and security practices to help thwart future attack attempts.

While it's not clear if the library will need to temporarily close again to repair affected systems, non-traditional collections such as wifi hotspots, musical instruments and telescopes cannot be checked out at this time.

Library IT staff believes they were "targeted" in ransomware attack

By Jacob Mulliken Messenger-Inquirer Jul 23, 2019

1 of 2



Erin Waller, Daviess County Library Director

Maria Clark

Information technology staff at the Daviess County Public Library hope to have library patron operations up and running within the next two weeks, according to IT Manager Brian Lashbrook.

"My hope is that self-checks, patron catalogs, really all of it, will be up in roughly two weeks," he said. "The reason that it takes so long is that our vendors are on a project schedule, but they are traditionally good about bumping us up."

Lashbrook, IT Assistant Wesley Johnson and Information Services Manager Alicia Harrington have been working nearly non-stop with the aid of outside consultants and their various technology vendors to address the persistent issues resulting from the April 28 ransomware attack, said Library Director Erin Waller.

IT staff have been working with Innovative Interfaces, who provides the library's check-in and cataloging service Polaris, as well Bowling Green-based consultant Innovative Solutions Through Technology to address current issues as well as better prepare for the future, Lashbrook said.

"We are rebuilding everything from scratch," he said. "It is better safe than sorry at this point. We are taking every step possible to ensure that the ransomware is gone and that we can get back to running normally. We have to request server upgrades from Innovative Interfaces and they are working with us to move our data as we upgrade to Windows 2019. We have also set up at this point that all staff machines are unplugged from the servers and running off of a secured Wi-Fi connection as we address staff server issues.

"We have also set up a separate local area network to block any kind of traffic with anything that could be infected as we rebuild servers. We are upgrading to all of the current Windows systems and are going to begin setting all the staff computers to backup to OneDrive, so if something goes wrong we can grab it, wipe it, reload it and all of the data will come back."

While library officials are looking toward extra precautions, by virtue of the library's function in the community, patron restrictions will not be stringent, Waller said.

"Any of the extra precautions we have put in place are going to most likely add restrictions on staff itself," she said. "We don't want to be locked down like a hospital or a bank. Our staff needs to be able to access what they need in terms of catalog and patron information. We will do what we can, but we have to be cognizant of our jobs and provide customer service and access. We will definitely be boosting training initiatives for staff, just to remind them of what to look for."

One of the common ways that ransomware can enter into an individual computer or an entire system is through phishing emails that contain malicious attachments, or through drive-by downloading, which occurs when a user unknowingly visits an infected website and malware is downloaded and installed without the user's knowledge. Neither of those Lashbrook theorizes were the culprits.

"Most likely it came through a staff computer," he said. "The public computers are set to wipe everything out between sessions through a software we use called Deep Freeze. From what I have learned it seems like it most likely got in through the firewall somehow. A lot of them currently use a remote desktop and will set a bot and brute force the password until they get in. I was able to look at the way that it operated a little bit and it basically runs and tries to break the security on built-in Windows accounts and once it does that, it can reach out to any computer on the network using that password and account. I feel like we were targeted, that is my theory."

In terms of the library's IT departments current course of action, they aren't taking any chances moving forward, Lashbrook said.

"We have talked to a few different experts and the path that we are taking is the right way," he said. "If you don't have an idea of where it is hiding, you have to wipe the hard drive and start over. It is a long process, but we are focusing on critical services first, access to patron accounts, account services, and then we will focus on getting staff computers up and reloaded with backed up data. We aren't taking any chances this time."

The library was initially attacked on April 28. Their files were encrypted and held ransom by a form of ransomware called Cryptolocker for six bitcoins, or \$30,947, which the library did not pay. Ultimately, the library was forced to close its doors May 7-9 to address issues and have employees re-inventory its more than 300,000 items. The issue has been at the forefront of the IT department's duties this summer and has, in some ways, hurt the morale of both staff and patrons, Waller said.

"Brian, Wesley and Alisha have put in countless hours and have gone above and beyond the call of duty," she said. "Our staff have been great in creating and implementing creative solutions to ensure that our patrons' experience is as seamless as possible and our patrons have also been patient with us and supportive of our efforts. I can assure everyone that the security of our patrons is our top priority and that no patron information was compromised."

Jacob Mulliken, 270-228-2837, jmulliken@messenger-inquirer.com

The Week in Libraries: August 16, 2019

Among the week's headlines: a library receipt kicks off a debate about the value of libraries; more media coverage of the library e-book market; and the University of California holds firm in its negotiations with Elsevier

by Andrew Albanese | Aug 16, 2019

 [Comments](#)

 **SUBSCRIBE**
by the Month



State Library of NSW, via Creative Commons


This week, [a receipt from the Wichita Public Library went viral](#) after being posted

on **Reddit**. Through a feature provided by the library's ILS vendor, Polaris, the receipt for checked out items showed that a family of six saved \$164 on its recent visit (and more than \$1,384 this year alone) by borrowing materials during their weekly visit to the library. A pretty clever way to point out the value of libraries and their core mission of providing access to books and reading, right?

Apparently not: in a sign of the times, as **Yahoo News** reports, [the receipt instead sparked a debate about "the thousands of dollars" libraries are costing authors.](#)

RELATED STORIES:

- More in [News -> Libraries](#)

 [Want to reprint? Get permissions.](#)

"To hell with supporting authors," one commenter posted sarcastically.

"Sorry, but I'm not going to be spending \$10-\$20 every time I see a book I *might* be interested in," another commenter replied.

Meanwhile, another commenter succinctly summed up my reaction to the story: "People are actually debating the morality of using a library?"

FREE E-NEWSLETTERS

 PW Daily Tip Sheet**SUBSCRIBE**[More Newsletters](#)

In his latest ***Publishers Weekly*** column, [University of Washington iSchool professor Joseph Janes thoughtfully engages this very subject: the natural tension between the library and publishing worlds, through the lens of the increasingly contentious library e-book market](#). "It strikes me that the perennial question at the heart of the e-book debate predates and extends beyond the current state of the market: do publishers and authors see the library's relationship to them as more symbiotic, or parasitic?" Janes writes.

The long-running tension between publishers, authors and libraries is nothing new, Janes points out in his column. But in the still emerging library e-book market, where publishers hold all the cards in terms of licensing access, it appears to be escalating.

"Do I think that the major publishers are restricting e-book access because they don't like libraries? No," Janes writes. "What I do think, however, is that Macmillan and a few other major publishers' actions in the e-book realm are based less in reality than in a specific perception (or misperception) of reality. And I'm afraid that until a more accurate perception of libraries takes root among publishing executives, it's hard to see the library e-book market improving."

Despite recent actions, Janes remains optimistic that things can improve.

"I'll admit, it's hard not to wonder who in publishing's C-suites today recognizes that libraries are not the problem—that libraries are in fact publishers' most steadfast partners in a literary ecosystem that, for generations, has fostered the highest-quality writing, generated sales, and helped society learn and grow," he writes. "But I am still idealistic enough to believe that we can have a constructive and meaningful discussion. And I believe that if we do that, we will find a way to accommodate everybody's interests—authors, publishers, libraries, booksellers, and, especially, readers. Remember them?"

Reserve Reading

One of the initiatives aiming to help publishers and authors get a better grasp on how library e-books benefit authors and publishers [is the Panorama Project](#), the OverDrive-funded library advocacy effort. This week, Panorama [announced its latest "Panorama Picks" list](#), a data-driven quarterly report on the "under-the-radar fiction, nonfiction, and young adult backlist titles" that library patrons are waiting to borrow. The lists are optimized for local interest via regional groupings aligned with the [American Booksellers Association's](#) (ABA) regional associations.

Another week, and more press reports about the difficulties libraries are facing in the e-book market: [Geekwire has picked up King County librarian Lisa Rosenblum's excellent explainer on Macmillan's two-month e-book embargo](#). "To understand the impact of Macmillan's decision, it must be put in perspective. Libraries maintain 'Purchase to Holds' ratios to minimize wait times for popular titles. As a large library system, KCLS maintains a 5:1 ratio. That means for every five holds placed on a title, KCLS purchases one copy to ensure a maximum wait time of three months. To illustrate, after months on KCLS' Top 5 eBooks list, the bestseller *Where the Crawdads Sing* by Delia Owens still has 1,848 holds on 372 copies. *Educated: A Memoir* by Tara Westover has 1,089 holds on 358 copies. If KCLS had been limited to only one digital copy of each of these high-demand titles and then had to wait eight weeks before being able to purchase more, the impact would be dramatic. Patrons could conceivably wait years rather than months for their eBook." But borrowing e-books is "frictionless," right?

[In Toledo, Ohio, a report on the local ABC affiliate](#). "Providing digital content is challenging for libraries on a number of levels. For starters, it is an expensive venture. Libraries pay 3-4 times what they would for a print title, and often they only get it for two years before having to renew."

And in Texas, the **Waco Tribune-Herald** [also has a report on the recent publisher changes for library e-books and audio](#). "It's going to affect us in certain areas," Waco-McLennan County Library Director Essy Day said. "The business model for e-books and e-audiobooks is horrible, in my opinion."

Via **Publishers Weekly**, [more digital content libraries will not be able to license for their patrons](#). Amazon's Audible division has entered into yet another deal, this one with Skybound Entertainment, to create multiple audio-only originals available exclusively to Audible subscribers.

The University of California is showing serious resolve in its pursuit of open access. In the latest development in its dispute with Elsevier, reported by **Science**, [some of the university's "most prominent scientists" announced they will resign from the editorial boards of Cell Press over the impasse](#).

Via **Publishers Weekly**, textbook publisher [Cengage is facing a new class action lawsuit from a group of its authors over the its switch from printed books to digital subscriptions](#). It's the second suit filed in just over a year, after a previous suit was settled last October.

Meanwhile, **SPARC** [has joined the chorus of critics calling for government regulators to block a proposed merger between Cengage and McGraw-Hill](#). "The merger would decrease competition, increase prices, and lock students into digital courseware that can gather vast amounts of their data," said Nicole Allen, Director of Open Education for SPARC. "It flagrantly exceeds market share thresholds established under federal antitrust law. The textbook publishing industry engaged in unsustainable pricing for decades at the expense of students, and eliminating competition adds insult to injury. This merger should not be allowed to proceed."

The New York Times reports that New York's [Culture Pass initiative, which gives local library cardholders free admission to a growing list of cultural institutions](#) (including the Metropolitan Museum of Art, and the American Museum of Natural History among the more than 50 partners) has been very successful, signing up more than 70,000 in year one.

Also, from **The New York Times**, [a look at libraries that are also tourist attractions](#).

A sad sign of the times in America, via the **local NBC affiliate**: [The Charleston Public Library will add armed guards](#). The move comes after "a shooting threat via email in October 2018" led to the temporary closure of several branches.

And via **19 News**, [a task force is considering security enhancements at the Cleveland Public Library following a shooting there](#).

The Guardian [reports that British bookseller Foyles is setting up libraries](#) in "high-end" retirement homes.

From **Vox**, a look [at Barack Obama's summer reading list. Which is awesome](#).

And, we know you love your local librarians. So, show 'em! Nominations for the annual [I Love My Librarian awards are now open](#).

The Week in Libraries: August 23, 2019

Among the week's headlines: why most authors are trying to get their e-books in libraries; the backlash continues over Macmillan's library e-book embargo; and publishers sue Audible over its Captions program

by Andrew Albanese | Aug 23, 2019

 [Comments](#)

 **SUBSCRIBE**
by the Month



In

Indie author Ran Walker (l.) and BiblioBoard's Mitchell Davis.

announcing [the publisher's two-month embargo on new release e-books in libraries](#), [Macmillan CEO John Sargent introduced a murky new metric for evaluating the library e-book business](#): revenue per "read." As [numerous observers have pointed out](#), that's problematic for a number of reasons. But fundamentally, Macmillan's focus on library "reads," librarians and indie authors say, discounts the greater asset libraries deliver: not reads, but *readers*.

RELATED STORIES:

- More in [News -> Libraries](#)

 [Want to reprint? Get permissions.](#)

FREE E-NEWSLETTERS

PW Daily Tip Sheet

[SUBSCRIBE](#) [More Newsletters](#)

Today I grabbed coffee with [BiblioBoard's Mitchell Davis](#) and [indie author Ran Walker](#), winner of [the 2019 National Indie Author of the Year Award](#) (selected by judges from *Library Journal*, *Publisher's Weekly*, IngramSpark, St. Martin's Press, and *Writer's Digest*). The author of some 16 books, Walker, a former lawyer who teaches creative writing at Hampton University in Virginia, told PW why he views libraries as integral to his success as a writer, not as a threat to his sales.

"I've had a lot of great experiences with libraries and I see the benefit for authors, and especially self-published writers," he says. "You want readers. And librarians are the main curators of literature. I think you do yourself a disservice to ignore libraries." Walker says he's followed recent

developments in the library e-book market, and doesn't quite understand Macmillan's decision to keep new release e-books out of libraries, especially for debut and mid-list authors. "It doesn't even make sense," he says. "Let's pay some respect to libraries."

Meanwhile, through Biblioboard and [the Indie Authors Project \(IAP\)](#), Davis has been working to make a curated selection of the best indie writers available through libraries in new and creative ways. [Working with OverDrive](#), the inaugural IAP e-book collection, released last summer, featured 50 select titles available through libraries via a simultaneous use, royalty-paying e-book collection. And the results have been impressive, with the collection clocking more than 200,000 circulations.

[Stef Morrill, director of the Wisconsin Library Consortium \(WiLS\)](#) said the collection did especially well with Wisconsin readers. Morrill told PW that WiLS had 19,312 total circulations of the 50 independent author titles in the Indie Author Project Collection in the seven months of 2018 they were available via WiLS's OverDrive collection, an average of 386 circulations per title.

"If we translate that to a one copy/one user model, with each copy circulating two times per month, which is high, we would need approximately 25 copies per title to meet this demand, 1,250 copies total," she says. "That's a lot of copies."

Morrill said the IAP collection's success has helped open her eyes to the wealth of good authors now working outside the traditional publishing channels. And while Morrill says that WiLS will always look to offer patrons access to the most in-demand e-books from the major publishers, she conceded that the level of reader satisfaction with the IAP collection, along with strong circulation numbers, and the chance for the library to better optimize how its collection budget is spent, means that indie authors (like Ran Walker) eager to partner with libraries could soon earn a larger cut of the library e-book market.

"It's very interesting to consider: what is really so different about this indie content? And, what does it mean to be published these days, especially with Amazon now publishing so many books," Morrill said. "The market is changing and it is changing fast, and the decisions being made by the major publishers in the e-book market are going to force libraries into some decisions. As a statewide consortium, we spend over one million dollars a year on OverDrive content. And we're going to be having discussions through the fall about what we want to support with that money."

Reserve Reading

Local media continues to pick up on the Macmillan embargo and the changes in the library e-book market. Via the *Dayton Daily News*, Tim Kambitsch, Executive Director of the Dayton Metro Library, [suggested that libraries need to better engage with publishers, suggesting that Macmillan's recent changes were "a good illustration of them acting in a vacuum."](#)

Kambitsch is also quoted in a report on Dayton's *WDTN-2* news. [Speaking of a vacuum](#): "2 NEWS emailed Macmillan Publishing on Monday requesting comment or an interview, but as of the publication of this article, had not heard back. Kambitsch said several top state and national library associations have also tried contacting Macmillan, and haven't heard back."

Cincinnati Public Radio warns that ["Library Wait Times For E-Books, E-Audiobooks Are About To Get Longer" in its report.](#)

In Arizona, *KOLD-13* [reports that publishers "are making e-books harder to get."](#) According to one Pima County librarian, "we may have to buy less e-books and more physical copies, or we may have to let the holds increase." [A note on the Pima County library web site urges patrons to get involved.](#)

And in Michigan, Valerie Meyerson, director of the Petoskey District Library, penned an editorial in the local **News-Review**. "[The publishing industry now has almost an adversarial relationship with public libraries](#)," she writes.

As **PW** reports, The Association of American Publishers [filed suit against Amazon's Audible division today](#) in the U.S. District Court for the Southern District of New York, seeking to enjoin Audible from moving ahead with a feature, called [Captions, which would scroll computer-generated text with digital audiobooks](#). Though the feature hasn't yet been rolled out in the market, AAP is asking for a judge to enjoin Amazon from the unauthorized display of text. All the Big Five publishers have signed on to the suit, as have Scholastic and Chronicle. "We are extremely disappointed by Audible's deliberate disregard of authors, publishers, and copyright law," AAP president and CEO Maria A. Pallante said in a statement. "In what can only be described as an effort to seek commercial advantage from literary works that it did not create and does not own, Audible is willfully pushing a product that is unauthorized, interferes and competes with established markets, and is vulnerable to grammatical and spelling inaccuracies—it is a disservice to everyone affected, including readers."

The Verge, [meanwhile, points out that "the case has a strong analog to a former Amazon publishing controversy a decade ago](#), when the company tried to launch a text-to-speech feature for its Kindle platform that would effectively do what Amazon Captions does today, but in reverse." [Except, of course, that program never actually launched, and no suit was ever filed.](#)

The New York Times [reports that "state attorneys general in more than a dozen states are preparing to begin an antitrust investigation of the tech giants."](#)

And, also from **The New York Times**, [a group of four prominent antitrust experts explore what action against the tech industry might look like.](#)

On the open access front, [via InfoDocket, Springer Nature has announced a major deal with Projekt DEAL](#), a consortium of more than 700 publicly and privately funded academic and research organizations in Germany, which will mean "substantially enhanced access to Springer Nature content for almost all of the German research landscape."

In **The Atlantic**, [a former federal prosecutor offers an interesting primer on free speech.](#)

Ah, the digital age: As libraries gear up for the 2020 census, **Wired** [offers a cautionary essay on what could lie ahead](#). "When the census arrives, so will cyber scams: phishing emails from bad actors claiming to be bureau representatives, text messages with malicious links, and harassing phone calls demanding private information," the article notes, adding that among the most widespread scams "may be ransomware at public libraries," which could temporarily halt internet access and cripple the census, which for the first time will have an online component. "Twenty percent of Americans—about 66 million people—don't have home internet access, which is exactly why the [Census Bureau] encourages going to public libraries to fill out the 2020 Census," where libraries will offer "internet-connected desktops and designated census kiosks." Unfortunately, the article points out, "cyberattacks on libraries continue to wreak havoc across the United States." Russia, if you're listening...

Make of this what you will: **Town & Country** [has a piece on Gwyneth Paltrow's "personal book curator."](#)

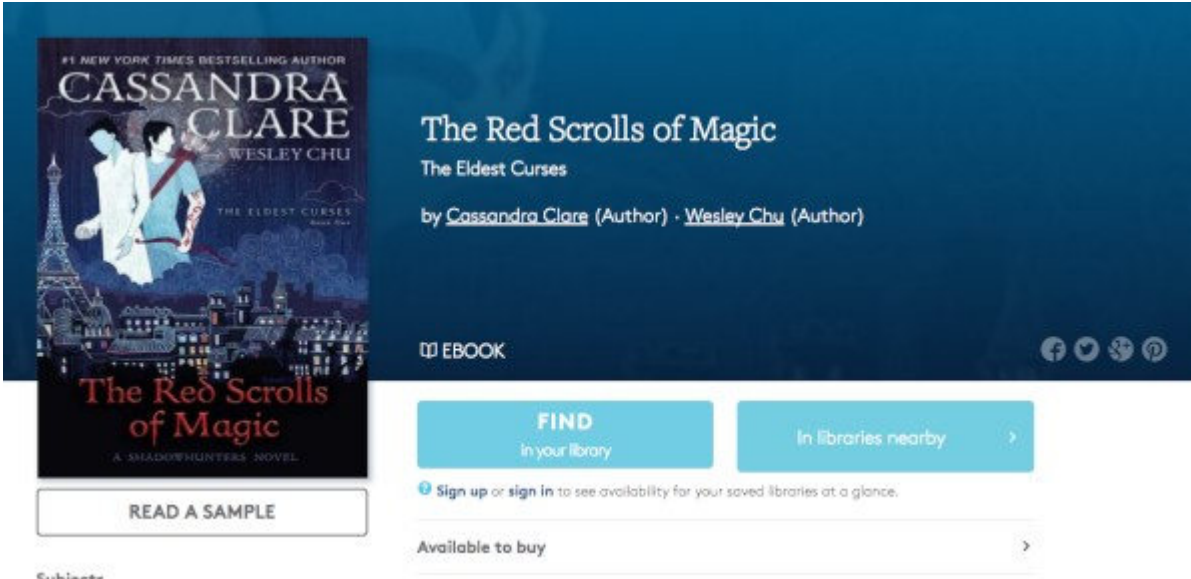
The Week in Libraries: September 6, 2019

Among the week's headlines, sticker shock over S&S's new library e-book prices; ALA organizes a national campaign against Macmillan's e-book embargo; and what's the future of school librarians?

by Andrew Albanese | Sep 06, 2019

 [Comments](#)

 **SUBSCRIBE**
by the Month



The Red Scrolls of Magic
The Eldest Curses
by [Cassandra Clare](#) (Author) · [Wesley Chu](#) (Author)

EBOOK

FIND
In your library

In libraries nearby

Sign up or sign in to see availability for your saved libraries at a glance.

Available to buy

Macmillan's controversial two-month embargo on new e-book titles in

OverDrive

Under Simon & Schuster's new terms of sale, the library e-book edition of 'The Red Scrolls of Magic', book one in Cassandra Clare and Wesley Chu's bestselling Eldest Curses trilogy, has doubled from a one-year to a two-year license—but librarians say the license cost has nearly tripled.

libraries [remains the main focus of librarians' displeasure](#) this week (see below), but another Big Five publisher is also drawing the attention of librarians. The changes to Simon & Schuster's previously announced digital terms of service kicked in on August 1—and librarians in the U.S. and Canada report they are discouraged by the publisher's price increases.

RELATED STORIES:

- More in [News -> Libraries](#)

 [Want to reprint? Get permissions.](#)

FREE E-NEWSLETTERS

PW Daily Tip Sheet

SUBSCRIBE [More Newsletters](#)

Price increases were expected—in [its July announcement, S&S was clear that most “new release” e-books would be priced between \\$38.99 and \\$52.99.](#) But with the new pricing now in place, and in some cases more than double the previous prices, are librarians experiencing a case of sticker shock?

In a pair of posts on the [Readers First blog this week](#), St. Mary's County librarian Michael Blackwell reiterates that not all of S&S's recent terms of sale changes are unwelcome—the publisher's switch from mostly one-year licenses to two-year licenses has been generally well received. The addition of a pay-per-read option for a publisher-selected group of S&S titles shows that the major publishers are capable of offering multiple models, the kind of flexibility that librarians have long been asking for. And librarians especially appreciate that S&S has committed to keeping digital content available to libraries upon publication—no embargoes.

Still, the price increases for many titles in the OverDrive catalog, Blackwell told PW this week, are causing concern among librarians. For example, [he notes](#):

Bob Woodward's *Fear: Trump in the White House* was previously priced at \$20.99 for a one-year license and now lists for \$51.99 for a two-year license.

Doris Kearns Goodwin's *Leadership: In Turbulent Times* has gone from \$20.99 for a one-year license, to \$59.99 for 24 months.

Lisa See's *The Tea Girl of Hummingbird Lane*, previously \$19.99 for one year, now is listed at \$59.99 for two years.

And, Cassandra Clare and Wesley Chu's bestselling *The Red Scrolls of Magic*, book one in the Eldest Curses trilogy, has gone from \$18.99 for a one year license, to \$51.99 for two years.

Blackwell also points out that some S&S titles which were already available as two-year licenses have also roughly doubled in price without additional time being added to the licenses—a straight up price increase. For example, Tony Robbins' *Awaken the Giant Within* was previously \$28.49 for a two-year license; it now lists for \$55.99 for the same two-year license. Rhonda Byrne's *The Secret* was \$23.99 for a two-year license; it now lists for \$47.99 for the same term.

Some of the increases are even more notable in Canada. For example, Robert K. Tanenbaum's *Capture*: was previously \$32 for a one-year license and is now \$119.99 for a two-year license, reports Toronto Public Library's Susan Caron, who shared with PW a list of similar examples.

Digital audio list prices have largely remained the same—however, titles previously were licensed on a perpetual access model. Now, they are now metered, and must be re-licensed after two years. Of the Big Five publishers, only Hachette and S&S currently meter digital audio licenses to libraries.

S&S's new prices and terms, it should be noted, are fairly standard among four of the Big Five publishers, and, in fact are often a bit less expensive (of the Big Five, only HarperCollins offers libraries digital access via a bundle of 26 lends, rather than a time-based license).

In S&S's specific case, librarians say they generally prefer to license access for more than a year. But they also note that checkouts for most titles tend to slow in year two, meaning that libraries are now being made to pay more up front in exchange for a second year of access which, their data shows, will often not be used. The net result: inefficiency for library managers, and less choice and longer wait times for readers, as more library dollars necessarily flow up to meet bestseller demand, leaving less money to take chances on new and mid-list authors.

Reserve Reading

In a press release today, **ALA** announced that on September 11 it will unveil "a public action campaign opposing arbitrary restrictions to library e-book lending," in response to "Macmillan Publishers' new policy" which embargoes new release e-books in libraries. "National library leaders including Kent Oliver, library director, Nashville Public Library; Mary Ghikas, executive director, American Library Association; and Ramiro Salazar, president, Public Library Association, will share library and reader impacts of the embargo and efforts to increase digital access for all." The announcement coincides with the 2019 Digital Book World conference in Nashville. The event will take place at the Nashville Public Library, 615 Church Street, Nashville, Tennessee. 2019, at 11 a.m. We will post more details as they become available.

Meanwhile, in her most recent editorial, *Library Journal & School Library Journal* editorial director Rebecca Miller [joins a rising chorus of librarians urging Macmillan to abandon its planned two-month embargo on new release library e-books](#). "This type of embargo can't be accepted as a new low bar," Miller writes. "Access to

readers shouldn't be viewed as a zero sum game. It's in everyone's interest to foster more readers."

American Libraries [highlights a selection of ALA award-winning librarians.](#)

Citylabs explores "[The Decline and Evolution of the School Librarian.](#)"

And, in the local **Lancaster Online** (PA), [a nice Q&A with Hempfield School District library department supervisor on the role of school libraries.](#)

Via Gary Price at **InfoDocket**, [the global "digital divide"](#) (the gap between underconnected and highly digitalized countries) will worsen if not addressed, according to the first-ever [Digital Economy Report](#), which calls for "concerted global efforts to spread the wealth potential to the many people who currently reap little benefit from it."

From the **Scholarly Kitchen**, [as the open access movement accelerates, Roger Schonfeld raises a provocative question](#): "Many libraries are using a negotiating playbook that would, if successful, prop up the big deal in this moment of disruption. Is this the best approach for the academy?"

From **The Washington Post**, ["New York is leading a multistate investigation of Facebook for possible antitrust violations, Attorney General Letitia James announced Friday, kicking off a bipartisan wave of independent state inquiries targeting the social media giant as well as Google's parent company, Alphabet."](#) Buckle up.

The Week in Libraries is a weekly opinion and news column. News, tips, submissions, questions or comments are welcome, [and can be submitted via email.](#)