Measuring Library Vendor Cyber Security: Seven Easy Questions Every Librarian Can Ask
http://journal.code4lib.org/articles/11413

By Alex Caro and Chris Markman

This is a simple grading rubric you can adopt or modify to help take this first step towards securing your library data. It is intended to be used by both technical and non-technical staff as a simple measurement of what vendor agreements currently exist and how they rank, while at the same time providing a roadmap for which security features or policy statements the library can or should require moving forward. More at: http://journal.code4lib.org/articles/11413.

Criteria	Brief Description	Point Value
1. Data Breach Policy	Is there a formal process in place to report data breaches if/when they occur?	+/- 1 point
2. Data Encryption	If patron data is stored by the vendor, is it encrypted?	+/- 1 point
3. Data Retention	Does the vendor purge patron search history records on a regular basis?	+/- 1 point
4. TOS "Ease of Use"	Can the average patron read and fully understand the vendor's terms of use policy?	+/- 1 point
5. Patron Privacy	Does the vendor use Google Analytics or other tracking software to monitor users?	+/- 1 point
6. Secure Connections	Does the vendor's website enforce secure connections only? (HTTPS or better?)	+/- 1 point
7. Advertising Networks	Does the vendor's website participate in ad networks?	+/- 6 point
	TOTAL POINTS	

Grade Scale:

A	Greater than or equal to 11 points
B	Greater than or equal to 10 points
C	Greater than or equal to 9 points
D	Greater than or equal to 7 points
F	Less than or equal to 6 points

1. Data Breach Policy

This is an interesting moment in time for libraries in the USA, because while some states have adopted data breach policy requirements, there is no federal mandate. So for example: let's say for a moment that the service provider your library uses to stream audio content experiences a *known* security breach and they have reason to believe customer information (including patron borrowing history) was compromised by a cybercriminal. If the vendor does not have a data breach policy, they have not made the commitment to inform users of their system when an event like this occurs, and you cannot make an informed decision about the overall performance of their security practices

because they have not stated they will voluntarily disclose this information. Vendors in this category receive +1 point if they have a data breach policy in place and it meets the criteria of the library, 0 points if no data breach policy is available, and -1 points if the data breach policy does not meet the library's criteria.

2. Data Encryption

The scary part about IT security is that we know no one is invincible—even three letter government organizations with monumental budgets experience security breaches. It isn't so much a question of *if* your systems will be attacked, but *when* and *how*. Done properly, data encryption is a very simple step towards ensuring that in the event of a security breach, your patron information is not an easy target. One could argue that data encryption is pointless if patron data is anonymized but what we need to consider is the fact that very often this type of information is used by cybercriminals in aggregate form to aid in future attacks. Data encryption is a very simple step to take and a nod towards some form of cyber security oversight by your vendor. Similar to the first criteria, vendors receive +1 point for data encryption, zero points if this information is unknown or unclear, and -1 if you can confirm they do not encrypt user data.

3. Data Retention

Many integrated library systems purge search history or user data automatically, but what about the systems they interact with? The point of this category is to make no assumptions—have you asked what their data retention policy is? Do they have one at all? What's an acceptable answer for your institution? Vendors receive a +1 if the retention policy is acceptable to the library, zero points if this information is unknown, and -1 point if the retention policy is deemed unacceptable.

4. TOS "Ease of Use"

"Terms of Service" (TOS) statements are typically written by lawyers, and are not only extremely difficult to understand, but frustrating to read due to their length. An unfortunate side effect of this is that many users simply click past them, without reading the fine print. It's important for libraries to encourage users to read TOS statements because this empowers people to make informed decisions about how and when they want their personal information used. Some many not care, some may care a great deal, and some may care a lot more if they fully understood what information they were agreeing to hand over and how it could be used. Vendors receive a +1 if their TOS is easy to read, zero points if a TOS cannot be found, and -1 point if the TOS is difficult to read.

5. Patron Privacy

This category is specifically about "click-tracking", or background systems like Google Analytics that work invisibly on websites or web resources to collect statistical information about what pages are visited, for how long, and how they were located. *Many* websites use these tools, and their utility within library systems is an ongoing debate as we balance the needs of reliable metrics with patron privacy. The simple truth is that the most secure option is to disable these tools completely, or severely limit their use (perhaps stated in the vendor's data retention policy, or terms of use). Vendors receive +1 point if they respect browsing privacy, 0 points if this tracking is deemed within reason (for example, results do not include IP address), and -1 point if their use of tracking is not acceptable.

6. Secure Connections

All of the categories thus far have dealt with data "at rest"—information stored on hard drives or other media. In this category we're asking you to evaluate data "in transit", or en route to other computers (either library owned, or patron owned). It is laughably easy for even novice cybercriminals to detect unencrypted data passing through a network, and there are free software tools that do all of the work in that regard.Although secure connections are not the "final" solution to data security because protocols like HTTPS can be decrypted at the firewall level, much like category 2, it's a simple step to take. Vendors receive +1 point for forcing secure connections on their networks, zero points if this information is unknown, and -1 point if their connections are unencrypted / unsecured.

7. Advertising Networks

The scary part about a vendor's participation in or use of advertising networks is that you now need to consider not only your 3rd party vendor's security infrastructure and its relationship to your library CSRM, but also their advertiser's infrastructure. Also consider the fact that many ad networks re-sell their information to other advertisers, an action which you have no control over because they signed agreements with your vendor, not directly with you, the library. That is why this final criterion outweighs 1-6: participation in ad networks renders everything else moot if your vendor is doing the right things and then handing off the same patron data to an advertiser network with no relationship to the library or specific agreements about data retention or encryption. Not only that, but in recent years, cyber security attacks have actually been launched by cybercriminals *through* existing ad networks. We encourage you to use your best judgment in this category, because all ad networks are not alike, but ideally they're not something you should need to consider at all. For this reason you can award +6 points for non-use of advertising networks, zero points if it is unclear, and up to -6 points depending on how advertisements are used.