June 9, 2020

Open Sesame: Creating Stricter Evergreen Login Requirements for Staff and Patrons

>> DEBBIE LUCHENBILL: Welcome to the next session, and we want to give a big shout out to Equinox sponsoring our closed captioning and thank you to our awesome Captioner is doing a great job. I would like to introduce just Jessica Woolford, Amy Terlaga and Carol Yarrison, take it away!

>> JESSICA WOOLFORD: Thank you, Debbie. No. That is okay.

>> DEBBIE LUCHENBILL: I can see it.

>> JESSICA WOOLFORD: It keeps telling me I can't do it, anyway [Laughter].

>> DEBBIE LUCHENBILL: Yes I can see the whole slideshow.

>> JESSICA WOOLFORD: I control the screen but I cannot turn on my video.

>> CAROL YARRISON: That is for me also.

>> DEBBIE LUCHENBILL: Let me see if I can figure this out [Laughter]. Just a second.

>> JESSICA WOOLFORD: I can start talking even though you can see me --

>> DEBBIE LUCHENBILL: You should be able to do it now.

>> JESSICA WOOLFORD: Yay! hi, everybody peered welcome to our presentation I am Jessica Woolford and joining the are Amy Terlaga and Carol Yarrison we are from Bibliomation, and this

is the first time I presented with my coworkers. we are Connecticut's largest library consortium and very diverse library consortium with 63 public libraries ranging in size -- ranging in size from urban, multi-library system with several branches and from tiny little rural libraries one of which is not even have a bathroom. We have 7 K-12 school libraries in three special libraries which is a new thing for us, two that do not circulate new materials in one's --a historical society and that one is a maritime museum and the other that circulates is a church library. All very unique situations. [Laughter].

First, I want to talk about why did we feel the need to change the way that we were handling staff and patron logins. The first thing that was happening is as we were talking and gearing up to switch over to the web clients, the library started to be concerned about the security of accessing the web clients, if I can just click on the URL, and start using the system, what protections will they be in place to make sure that anybody can do that? They also were starting to get a lot of questions about patron IVA see at the same time. And because of the leaks and things happening, people getting into different systems to get personal information-- there is a big concern about that. Everyone was sharing the same password for at least two decades [Laughter]. So as Victor Hugo says in the quote here this is an idea whose time had come [Laughter]. We really needed to make changes and why not before we moved to the web client seemed a good reason as any to change the practices. We wanted them to switch to using -- Joe Smith if he wanted to access the library, he wanted-- we wanted him to use his own log in and password so if he went to another location or did not work at the library anymore we could delete the account or change the password and he would not have access to that account anymore.

We also wanted to change the way we handled permission groups. We had an approach that all users had -- even though they were, the username was done by name or function of the login, really, because we have such small libraries where everybody does everything, we could not just make those -- a cataloging only. We want to change that and make it so if you were a circ person you got circ permissions but not necessarily catalog permissions if you were technical services person that you didn't really do much with circ we want to make sure you had permissions appropriate for what you have been trained on for your job. We also decided to ramp up the security a bit to only give the register permission or register workstation permission to a select few in the library so that there only a few people that could register workstations and we figured they would not really need to do that often unless they got new equipment or switching from -- over to the web client, that is where they might need it but you're not going around registering a lot of work stations that prevented staff from being able to go home and login and look things up where they might not have wanted their stuff to be able to do that.

Nowadays in the post COVID world [Laughter] we have relaxed out a bit because we have library staff working from home good and we did give that permission to the higher tiered staff user accounts.

We also wanted to create an ability if staff had the desire to do this -- to manage their own staff user accounts. So there is only a few select individuals in library that can do things like change permission groups and register new staff accounts and delete staff accounts. We also wanted to try to change the way we handle passwords.

So we wanted all our users and staff and patrons to have a minimum 12 character password. This was something heralded by John Merriam, or Evergreen system specialist at the time, we really wanted stop -- we had been using the four digit, the last four digit of the telephone as the default password, but we wanted to get away from that and make things a little more secure for patients and staff.

We want to roll out the changes in stages for the libraries instead of cutting everybody over at once, we figured that would be too big a load on helpdesk. And also confusing for the libraries to do all at once. So we wanted to be able to do this in a managed way.

We wanted to get this all done before we started using the web client [Laughter], and we also wanted to get it done before I gave birth [Laughter]. I had a lot of projects that we wanted to get done for them, one of which was an upgrade, another one of which is this and we started this project in June 2018, I believe, and I was due March 25 of 2019, so we wanted to at least get the prep so I could hand it off to everybody, I want to go have a baby now [Laughter]. What do all staff need and what to do.

We had several meetings and the cataloging specialist apartments and the circulation. departments and what would be a permission that everybody needed, so the blue stuff is stuff that we decided that everybody needed. There were a few things we decided that nobody needed. The blue stuff is administrator stuff. The green is catalogers the yellow is circulators and we highlighted things we needed testing.-- The white stuff is the stuff we decided that everybody needed. I will go back to presenting.

These are questions we came up with one trying to figure out how to do this. What about small libraries were everybody does everything? Or tech services staff at work at the circ desk. If we needed both cataloging and circ permissions we would give you two separate permission group so we would use the secondary permission groups feature to give you additional permissions to do your job.

Another question what about part-timers that only need limited permissions? We didn't really know what libraries considered limited in terms of permissions. We sent out a survey to figure it out and what we found out was that everybody has a different definition of what limited meant so we decided to create -- BRE had a restricted staff permission group trees so we created limited groups based on the responses the library gave us from the surveys and gave permissions to those groups based on what the libraries wanted uniquely. Sensitive allowing staff to assign or grant permissions to users individually, there's the ability and evergreen but we decided the easier for us to manage, assign permission groups instead of assigning individual permissions and decided it would be easier for the libraries to understand then to be looking for the big permissions list which we had already done, and assign and grant things as needed.

This was, I apologize for the closed caption is because this is what I thought of later on that we did mention in our original presentation. What do we do about the old user accounts, the shared user accounts where we decided we were insecure and would not use moving forward? We decided once the staff had a chance to really test this stuff and merge them with the new user account, and the account we would merge, the old accounts with would be chosen by the libraries and Amy will talk about that more in her part, but I wanted to be mentioned here as well.

This is a picture from the GUI, the Evergreen staff client GUI. Of our old staff account tree looks like. It was, we kind of were using the stock thing that shipped with Evergreen but there were a couple things we added that were custom like the media specialist rebut we were really only using four of these. So we're using acquisitions, cataloger, circulator and media specialist.

We decided to keep that tree active while we were transitioning over, so staff could use their shared account logins at the same time and they were getting used to using their new account logins. We ended up with our new tree, so as I said before when we went through the list some permissions still fall under the regular staff umbrella, and for the rest of them these are just sort of unique groups that had unique permissions. For most of our permissions they were inherited on the previous slide. Staff accounts group there is. I ended up doing SQL to copy all of those

permissions into the regular staff tree. And took away stuff did that for most of the groups. That for acquisitions, cataloger, circulation and the school library staffed and decided we didn't want to have and want them to use secondary permission groups he did everything the library so we wanted them to make it simple as possible. School library staff have all the permissions they've ever had. Everyone else is more unique stuff. So it was easier to copy all the permissions we had and take stuff away than to start from scratch. There are so many permissions. The exception to that, the new groups, the local user admin and local workstation admin because the only really needed, these would be add on permissions anyway. And the only really needed certain types of permissions for those particular user groups.

With testing those, we figured what the minimum was. For the restricted tree, this used to be its own tree it was separate and under the users umbrella but we ended up having to move it new staff accounts umbrella and because we found out -- the way our old rules are written, we cannot place holds or these users could not place holds unless we were adding lately new rules to the system, we wanted to make it as simple as possible for that so we put them under the new staff accounts umbrella and made this subtree very limited that it had but I use the same approach in copping the permissions over and taking away what the library did not want these users to be able to do.

And, in order to make this work, we had to add new permissions so that staff could add new people to the groups. And those permissions are listed here. If you are interested.

So, following all the analysis we did some in-house testing, the consortium staff, we treated it as an upgrade without any of the new features. Without the fun stuff. But we tested the functions, checking things in and out, adding items and we had each department focus on their specialty. That went well. We found a lot of things that needed to be updated based on that testing. We added new permissions so the accounts could function properly. And through the testing we found we needed to add hold-- hold rules for the new account so they could place holds on the behalf of patrons. And we identified missing permissions.

I will turn it over to you, Amy.

>> AMY TERLAGA Hello everybody, I want to start by saying there is a Brady Bunch episode that if you watched a bunch you might remember it, Marcia Brady had to make a presentation

and she was anxious about it and her brother suggested she picture the audience in their underwear [Laughter].

I'm finding this is better because you don't see the audience. It's kind of freeing. [Laughter]. So testing, testing, testing. What we wanted to do is before we started rolling this out to all the librarians en masse we want to make sure it would work, so we approached five libraries. They ranged in size and we have a good mix of small medium and large. we chose them to give us good feedback and we also chose them because we knew the library's would roll with the punches we didn't get things exactly right and there were hiccups along the way, these librarians we knew would not freak out on us basically.

And so I think that's even more important in dealing with librarians and testing. We called them individually to talk about expectations and the process of what we wanted them to do. We need to make sure were accounting everybody the library and the permissions would do for them what they needed them to do. This is what we had for requirements. What permissions, in a Broadway, we didn't list out every single permission -- but it gave them a an idea of what they were signing up for.

Add staff accounts, delete accounts, that sort of thing. Even though we talked about it, I would have to say the majority of the library-- librarians want us to manage it. And so since we have switched them over to individual accounts, I would say there's a bit of activity there because what I did not realize was how many times their staff turnover at libraries, I did not realize that. We are creating accounts for librarians and deleting accounts on a regular basis. We also wanted to know who was going to register their workstations, I think Jessica mentioned this that we left it to just-- to her library because it is a security issue.

There are some protections, if someone quits the library is supposed to inform us so we can delete the account. So the ability to register workstations would mean they could go home theoretically and register. Also, who at the library would receive historical data from the current staff accounts which happened when we emerged old accounts into the new accounts. And then of course the setup of the limited circulator accounts as needed. There's a handful of libraries that use these limited circulator accounts for staff. Next -- slide. This is the basic form to use with the librarians to figure out what they needed. And it worked very well.

There were not too many times where it was like, oh, no, that is not what we were expecting to get out of this -- filling out the forms. Once the accounts were received and new accounts created, we generated these passwords for the librarians to use with the staff accounts. With the understanding they could change them if they found it was to -- if it was not memorable [Laughter]. We found a lot of librarians held on to the random passwords. John Merriam, who Jessica mentioned earlier, was working in the Evergreen department and did some programming and so he had come up with his own random password generator that we used and there were three words at random separated by spaces. They worked extremely well. And then when the libraries were contacted, we shared with them the transitioning to the user accounts document which -- trying to cover everything the library would bump up against, say you started using a new staff accounts -- for instance, how to change your password, the interface columns they had been used to with the size and how to deal with that. How to export and import your Cagle--- cataloging templates. Everybody needed to know how to do that so instructions on how to use that. Copy buckets. And reports, the report templates --

>> JESSICA WOOLFORD: It looks like the screenshots didn't come over.

>> AMY TERLAGA I see. So how to share report templates because when the old accounts are merged into the new accounts, report templates made it over to just one individual. You would want to know how to share those report templates when the accounts are merged.

>> JESSICA WOOLFORD: I'm learning how to do the keyboard shortcuts [Laughter].

>> AMY TERLAGA [Laughter] next slide. This was just one example of John's random password generator. So you didn't like it you just clicked on new password and then you would get another one -- Mary Assange selection list. Acquisition selection list. Yes, that is also -- that has to be moved over. So again, this worked really well -- it was a lot of fun actually [Laughter] you take your phone where you can get it and coming up with -- some of these random passwords were really surprisingly humorous so yes, we did that for a lot of libraries. We encrypted the documents and sent them to the libraries, and I would talk to library directly and give her the password to unlock the document. Libraries tested for a period of one month, the good news is Jessica had done enough of the prep work leading up to this time, Carol?

>> CAROL YARRISON: My job is to create the accounts for the staff members. This is an example of one of the forms that would come back to Amy, she would pass it to me and I would

create the individual staff members accounts so they could log in to Evergreen. You can see where the libraries would identify what permissions we were going to need. They're using the first name and full last name, that is the-- where we went to Crete the barcoding username and sometimes we ran into the problems of the patron that created a username and that same format. Yet to find a username, new username and barcode to use but using the password generated we created a password and we used the real name of the staff member.

The secondary groups which we will talk more about later, we would put in as the libraries -- what I did is I did them in alphabetical order, sometimes it created issues if they wanted to do cataloging in their first group was acquisitions. We are still playing with that to see if it had any real function or any mishaps going on with that. We would get rid of the mailing address because for the staff member it wasn't necessary to have the mailing address. Some staff members do not have an email address either but we're going back and forth on that so to be quite honest, we have some with and without email addresses. For us, in Connecticut, residency is a requirement for a staff password. So the residents have to fill in where the staff member is working and it should be the same as the home library on the registration form. It's a long listing we have for 169 towns but not all the towns have their own library and some towns have more than one library. In order to get there perks from the state library, Connecticut is fortunate that they will allow out-of-town residents to use a library and the library is compensated for that privilege.

After creating the patron record I would go to other, and find patron or staff member rather permission to work in that particular library.

This is an example of a staff member at Bethel public library, scroll and fund the library they would be working in and go down to the end of the list and save it. It is a long less. I would go back in and find the patron through using the barcode I had created, and in patron search find the patron. And then bring up the secondary groups and assign the other groups they would need. On the initial creation of the staff member, you can only use one permission group read then you have to go back in and put in the secondary groups later.

This is just an example of the different user groups Jessica was talking about earlier. We had five. Again, I would put them in in alphabetical order so it would be acquisitions, catalog, circulation, local user and local workstation and sometimes it would make a difference as to what the staff member wanted to use but like I said, we are still working on that.

>> JESSICA WOOLFORD: I think that is the end of your stuff, Carol [Laughter].

>> CAROL YARRISON: I think so.

>> JESSICA WOOLFORD: Circling back around to passwords but once we had started to have staff transitioning to these new accounts, we really wanted to make sure they were not giving themselves a four digit password to log into the client, especially since we were giving that permission to some of the local people. We made a customization for the staff client and everybody was using Xul at this point but we did have both -- Xul and the staff client. Where the Mag John embedded his password generator into the patron registration form. That meant we have that requirement for patron spirit so when you click on the generate password button it would give you a three word password for everybody now.

We ended up changing the password length requirement people resetting your password through the OPAC, that was the first phase of this. Matt went fine. We didn't get too much pushback from the libraries about that, the board approved that one pretty -- quickly and that allowed us to have the longer password requirement for the staff and I think they realized the trade-off of that.

Then we wanted to take it a step further and say okay this is going all right, so what if we make that requirement for everybody? Including new patrons that come in or anybody that resets their passwords even if they are doing it at the desk. We put this before the board and the first reaction that we got is they had a lot of concerns about circulation staff being able to handle this change. They did not really want their circulation staff writing down a three word password and handing it to the patron. They figured what the-- if the -- patron loses it or the step number right to down wrong, there were things that could happen. We listened to those concerns and their concerns about his ability. Patron being able to sit down and type a password-- listen to the concerns and we decided not to put it up for a vote then but come back with a detailed proposal with something that might help the staff make the change. We used this famous comic. And the point of the comic if you have not seen this before, a lot of people probably have, the usual requiring numbers symbols in capital letters.

Actually it makes it hard for people to remember but easy for machines to guess. The point of this comic is that if you have four separate words, it becomes very easy for a person to understand or remember but more difficult for machine to guess. We did a demonstration on this using my password.net, and this was first brought my attention during a SysAdmin conference. Thank you for turning us onto the so I did demonstration -- even if I do ones that are different -- part of the keyboard, very easy for a computer to crack into that. We decided to go with three words instead of four to make it more palatable. So if I use four random words -- 10 billion years password.

We had to make changes to the code in order to make this happen. Changed the password hints here. We said, hey, if you are updating password and this is once user is logged into my account, it needs to be 12 characters in length and you can use a phrase, it you can use Makai don't say you can use basis but you can use a quote or it works in your favorite song.

We also changed the wording that happens, the password hints, so when you click on my account and go to login, it's as if this is your first time logging in please click here to set up your password. This uses the same form as it would use if you clicked on, forgot your password.

This takes it out of the library staff's hands entirely and it is something patients are used to, it is a self-serve thing now. It requires they have an email but, again, if you want to use an account online, it is pretty common for an email to be required.

We added that wording to the template. We also changed the password reset form so that we had more of a hint -- this is when you can expect the email to arrive because we have it set to run every half-hour so it could be up to that length of time before they receive the email. And if you've never signed before, we found that when the patient started using this more they were confused about the difference between a barcode and a username, so we had to tell them the number on your library card and we had to make it clear that they did not need to enter both because if they were entering some username that had not been used before, Evergreen would go, I don't know what that is and they would not get their email.

Some of the more technical changes we made to make this happen, this is information that John kindly provided to me so we could share it with you guys. We change the password in the-- account Perl module, so new password has minimum of 12 characters and no other symbols. We modified some of the JavaScript code so different password generation programs

were used to create that three word random password and the cool--- key there is that we had to disable the last four digits of the phone number was turned off.

The code John used to generate the password is a Perl script he wrote that creates those words from a dictionary file. Some naughty words had to be removed to make it usable for public consumption and occasionally you will see a phrase that is questionable we tell people if that happens to regenerate the password and no harm, no foul.

So John did say that if anybody's interested in that he would share that. So any password generator could be used as long as it is delivered to Evergreen correctly, John said and he used a CG wrapper around the Perl to deliver the password to Evergreen as a raw HTTP string and said that could probably be changed so the output is delivered directly to Evergreen but he thought that would be the quickest and easiest way to get a done at the time.

We are onto the question slide and I did want to highlight m that I did this year. This is my son on the day he was born. And this is him last week. So that is Philip and he was going to come to the live Evergreen conference with me so I thought this is the closest you guys might get to actually meeting him this year. There he is [Laughter].

>> CAROL YARRISON: I wanted to add something, if we have staff members working in two libraries, we had to create two separate accounts, one for each library. And the other thing we ran into was staff members would excellently emerge their personal accounts with their staff account that we created.

In order to get by that we had to put into-- put into the capital letters of staff with her last name with hopes they would not merge the two.

>> JESSICA WOOLFORD: Right. And we did have two, we had to add the word "staff" to the end of the last name and we did that for all the staff accounts so that we could know which account was there staff account -- when they looked -- at the patient search.

>> CAROL YARRISON: Why would you not want them to use their personal come for work, good question.

>> JESSICA WOOLFORD: I brought that up I think in an early meeting, we could have them use their personal or PL staff account and add stuff to it. --

>> AMY TERLAGA Some do, actually. I have seen that. Yes.

>> JESSICA WOOLFORD: I've seen them check out stuff to their staff accounts but I don't know, we thought some libraries would want to keep it separate and it might be confusing to untangle some of that stuff. I think that was the reasoning.

>> CAROL YARRISON: Right, Diane, that was something we had to explain to the staff members. Yes. The staff accounts are actually patron accounts. And they do get that confused.

>> DEBBIE LUCHENBILL: I think we are pretty much at them over there is another question that came in, did you encounter significant resistance to libraries in regards to the changes or resistance to doing the testing and if so how did you do -- make the case for the change?

>> JESSICA WOOLFORD: Is say that again?

>> ANDREA BUNTZ NEIMAN: Did you encounter any significant resistance to lovers in regard to the changes or resistance shooting the changing and if so how did you make this case for the change.

>> JESSICA WOOLFORD: Are we talking about for staff accounts at this point?

>> DEBBIE LUCHENBILL: I would guess so.

>> JESSICA WOOLFORD: We did have a bit of resistance to this because-- especially for the small libraries where they were used to making it simple and they had older staff members. I think the compromise we came up with for a lot of the staff was that if you want to have a shared account let's set you up with the limited user account so they have the ability to do the minimum you want them to do anyway and that has been working out well. I think that get over the resistance.

>> AMY TERLAGA We focused on that you do change operator and they had to keep logging out and logging in. That made a difference.

>> JESSICA WOOLFORD: Yes, most of the libraries didn't know that change operator feature existed till he pointed it out to them because white with date they were using the same account. I think someone also pointed out that the three word password opens up to dictionary attacks and that is something to consider going forward I suppose.

>> DEBBIE LUCHENBILL: Thank you all, that was really interesting. And thank you everybody for attending. The next session will start in five minutes. I will put up that slide. If you are not attending that session, please do log out of this track so we have enough seats for everyone. There is a discussion continuing on the chat and feel free to do that and we are continuing the track without stopping so we will see you again in five minutes.

>> AMY TERLAGA Thank you, Debbie.