In the digital age of legal research, the paradigm has shifted from the use of print resources to the use of online legal research databases. These databases require that users must first obtain a username and password before being allowed access to them. Law librarians in academic, government, corporate, or firm law libraries are responsible for creating user credential (access control) requirements, and for maintaining and troubleshooting user access to these legal research platforms. User issues include password fatigue (from entering different usernames and password combinations) and reduced productivity (due to time spent re-entering passwords for the same identity). In addition to these user issues, law librarians receive a significant number of inquiries related to password requests or blocked access. My library alone has received close to two thousand tickets this year related to password and access issues.

**Security and User Behavior**

Electronic Resource Management (ERM) providers TRG Research Monitor, ITS OneLog, and Lucidea LookUp Precision using new password management tools and single sign-on (SSO) authentication to increase security and provide a better user experience.

**BY ANDRE DAVISON**

**TALKING TECH**

**Powerful Password and Authentication Tools for Improving the Use of Online Legal Research Databases**

Image © iStockPhoto.com/Peshkova
SAML enables web-based security interoperability functions, such as single sign-on across sites that are hosted by multiple companies. Single sign-on (SSO) is an authentication process that allows a user to access various applications with one set of login credentials. SAML SSO works by transferring the user’s identity from one place [the identity provider] to another [the service provider].

SSO works by transferring the user’s identity from one place (the identity provider) to another (the service provider). A dependable directory service is a critical prerequisite for SSO. There are two primary access protocols to be aware of: Active Directory Federation Services (ADFS) and Lightweight Directory Access Protocol (LDAP).

Microsoft developed ADFS to extend enterprise identity beyond the firewall. It provides single sign-on access to servers that are off-premises. ADFS is a type of Security Token Service (STS) that uses a claims-based access-control authorization model. This process involves authenticating users via cookies and SAML.

LDAP is a lightweight subset of the X.500 Directory Access Protocol and has been around since the early 1990s. It was developed by the University of Michigan as a software protocol to authenticate users on an active directory (AD) network, and it enables anyone to locate resources on the internet or on a corporate intranet. LDAP single sign-on also lets system admins set permissions to control access to the LDAP database. That way, you can remain confident that data stays private. Whereas ADFS focuses on Windows environments, LDAP is more flexible. It can accommodate other types of computing, including Linux/Unix. LDAP is ideal for situations where you need to access data frequently but only add to or modify it now and then. LDAP works exceptionally well with passwords. It can deal with password expiration, password quality validation, and account lockout after a user has too many failed attempts. An LDAP agent also can authenticate users in real time. It compares the data presented to what’s stored in the LDAP database instantly, so no sensitive user data needs to be stored in the cloud.

Implementing SSO Authentication at Blank Rome
Westlaw, Lexis Advance, and Bloomberg Law all support SAML SSO authentication.

provide password management modules. These modules have features that collect credentials, auto-populate login information, and provide reports and login analysis. All of these products are great tools that help organizations with password management, but they don’t address security issues related to user behavior.

Here are the top three examples of user behavior issues we consistently encounter at Blank Rome.

- Users don’t log in to an online research platform for a specific duration and must reset their password.
- Users attempt to log in with the wrong credentials too many times and have their accounts locked.
- Users forget the answers to their security questions and have their accounts locked.

Security Is a Serious Concern When Dealing with Password Issues
In the data breaches that have occurred at eBay (145 million users), Adobe (36 million users), and JP Morgan Chase (76 million users), passwords were frequently the target. Law firms and corporations across the nation consistently deal with the risk of phishing. Phishing is the fraudulent practice of sending emails purporting to be from reputable companies to entice individuals to reveal personal information, such as passwords. Concerns about the reliability of username and passwords is not a new development. The topic was discussed back in a 1994 Washington Post article titled “The Secret Password is ... Obsolete” by John Burgess. Burgess opened the article with the statement: “Since the dawn of the electronic age, the computer password has been a trusted guardian of secrets large and small. For many people, obtaining their own password became a rite of initiation into computer culture itself. Now, growing numbers of security experts feel that the password in its common form is too old and unsophisticated for the job.”

In the 25 years since this article was written, technology has developed better forms of authentication. One such type is SAML SSO login authentication.

The Benefits of Single Sign-On (SSO) Authentication
Security Assertion Markup Language (SAML) is a language protocol for handling authentication and authorization in a network. In November 2002, the Organization for Advancement of Structured Information Standards (OASIS) ratified SAML as the eXtensible Markup Language (XML) framework for exchanging authentication and authorization information among business partners, particularly through web services. SAML enables web-based security interoperability functions, such as single sign-on across sites that are hosted by multiple companies. Single sign-on (SSO) is an authentication process that allows a user to access various applications with one set of login credentials.
Law librarians are well suited to aid in the battle against cybersecurity threats by supporting and protecting password practices.

SAML SSO was not painful to implement. Blank Rome had the technology in place for another application used internally. If you are interested in this process, I would recommend talking to your IT team to determine if your organization is currently using SAML SSO. Also, technical team members for the online legal research vendors are great resources to educate you on the SAML SSO process. SAML SSO could potentially eliminate passwords, increase security, and increase productivity at your organization.

**Final Takeaways**

- Law librarians have the skill sets to be great user experience designers. They can use technology such as SAML to improve accessibility to online legal research platforms.
- Law librarians are well suited to aid in the battle against cybersecurity threats by supporting and protecting password practices.
- Don’t let the acronyms intimidate you. Collaborate with your internal and vendor IT departments to understand the requirements to implement SAML in your organization.

---

**Implementation in Other Organizations**

Most colleagues that I have spoken to within academic and government law libraries are not exploring SAML SSO authentication. SAML SSO is more likely to be implemented in a law firm or corporate law library.

It is best to survey your stakeholders internally to determine if SAML SSO is a good fit for your organization. SAML SSO resolved most of the issues we experienced internally with our users. We are not able to measure the password fatigue for users but have received feedback on how efficient the new Westlaw login process is. We have also seen a reduction in the number of password and access tickets for Westlaw. We hope to have the same success when we go live with the Lexis Advance SSO and implement the Bloomberg Law SSO.

---

**Westlaw**

At Blank Rome, we have configured SAML SSO authentication for Westlaw. We worked internally with our IT team and externally with our Thomson Reuters technical client manager to set up SAML SSO. There are two ways for users to access SAML SSO. The first way is for users to click on a customized SSO URL to link your SAML account with your Westlaw OnePass account. Users then access SAML SSO by adding the customized SSO extension to their Westlaw URL to authenticate. Another option is for the user to click on the “Access with single sign-on” button and their organizational email address or group id. The benefits of the Westlaw SSO were immediately recognized. We were able to integrate the SAML SSO with our eLibraries. SAML SSO allowed users to bypass password authentication and client matter validation to take users directly to their preferred secondary sources.

**Practical Law**

We also implemented the SAML SSO authentication with the Practical Law Platform. Practical Law is a non-billable resource that resides on the Westlaw platform. SAML SSO users bypassed logging in to Westlaw and validating their client matter number to get to PLC (practical law). Users were taken directly to their desired PLC content by adding the customized SSO URL to the Practical Law URL. We customized links for the different Practical Law modules and added them to our intranet to provide convenient access to our users.

**Lexis Advance**

We have also configured SAML SSO for Lexis Advance. We went through a similar process of working internally with our IT team and externally with the LexisNexis staff field systems engineers. Users don’t have to initiate the SAML process in Lexis Advance manually. The LexisNexis team adds the users to SAML SSO access. We have not launched SAML SSO into production for Lexis Advance. LexisNexis is currently in the process of migrating all their ancillary products to the Lexis Advance platform and we wanted to wait until that was completed to put it into production. One advantage to configuring the SAML SSO for Lexis Advance was that we were able to configure SAML SSO for the Wall Street Journal easily. Blank Rome users experienced several issues with the Wall Street Journal enterprise access due to a security protocol that required users to reactivate their access every 90 days. We have not experienced these issues since we implemented SAML SSO for the Wall Street Journal.