Microsoft Secure Score: Lawyers Need to Know (and Improve) Their Score

by Sharon D. Nelson, Esq. and John W. Simek

Security should be top of mind for everyone today, especially given the tremendous increase of cyber attacks and ransomware infections since the pandemic. Lawyers hold a lot of confidential data that can be very valuable to attackers. It's not just data for one client, but data for multiple clients, which provides a one-stop shop for cyber criminals. What is a lawyer to do?

The first step is to assess your current security situation. A good beginning is performing a vulnerability assessment. Vulnerability assessments are not that expensive - even for the solo and small firm lawyer. Make sure you a quoted a flat fee that includes a report of your vulnerabilities ranked by severity so you know what to fix first.

As most lawyers are now subscribed to Microsoft 365, determining your Secure Score is another item to investigate.

What exactly is the Microsoft Secure Score? Simply put, it is a measurement of your security posture. If you are a gamer, think of it as a technology security game. The higher the number the better the score. Secure Score is now shown as a percentage of your points as compared to the total number of points available. Microsoft makes it easy for you to determine your Secure Score by providing an improved Microsoft 365 security center (https://security.microsoft.com/). Just login to the security center as an administrator and your secure score is shown right on the dashboard. Pretty nifty.

As Microsoft states, improvement actions are organized into groups.

- Identity (Azure Active Directory accounts & roles)
- Device (Microsoft Defender for Endpoint, known as Microsoft Secure Score for Devices)
- Apps (email and cloud apps, including Office 365 and Microsoft Cloud App Security)

You accumulate points by configuring the recommended security features, performing security-related tasks, or improving interactions with third-party services and applications. The more items you can check off, the more points get added to your score. See, it really is like a game.

We won't go into a lot of detail about specific items covered or which Microsoft products are included. At the present time, recommendations are provided for the following products.

- Microsoft 365 (including Exchange Online)
- Azure Active Directory
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Cloud App Security
- Microsoft Teams

Microsoft is continually improving Secure Score so check back **often** to see if other products you license are included in Secure Score. Don't forget that you also have the ability to indicate that you have

covered the listed item by using a third-party application. As an example, perhaps you are using a third-party provider for your MFA implementation. Secure Score can only provide real-time insight into products provided by Microsoft so you would manually indicate the third-party MFA provider, which will add the appropriate points to your score. That is also a nifty enhancement.

If you scroll down the dashboard a little, you will see a graphic section for comparison. Your score will be shown as well as the typical score for organizations like yours. This is a great tool to see how you compare to others that are similar in size utilizing similar services. While the true gamer will attempt to score all of the available points, the goal should be to constantly improve your score and be more secure than similar organizations.

Do not be discouraged if your Secure Score is under 50%. A Secure Score of 47% is pretty good if comparison organizations are only at 21%. Having said that, you really should try to achieve a secure score in the 60%-80% range in our opinion. A score of less than 60% probably indicates that some best practices are not implemented or configured. It is relatively easy to get to the 60% mark with a modest amount of effort. Getting to 80% is a lot harder. You will have to do more detailed work to get those last few percentage points.

You have a friend in Secure Score because it will helpfully give you recommendations to improve your score. The dashboard very conveniently shows you a list of top improvement actions with percentages indicating the score impact.

As an example, an improvement action may be to “Enable policy to block legacy authentication” with a score impact of 12.5%. Clicking on the recommendation takes you to a screen where you select the action plan (To address, Planned, Risk accepted, Resolved through third party or Resolved through alternative mitigation), what the user impact would be and the implementation steps to complete the recommendation.

The advice is to plan your improvement strategy. Update the various recommendations to “tag” those you plan to address in the future. This will give you a road map for improvement – just make sure improving your score remains on your task list.

Some lawyers will conclude that maintaining and improving their Secure Score is too complex and time consuming. Not a problem. **Make sure whoever supports your IT services knows what Secure Score is and how to improve it**. That could be your “secret sauce” to reasonably securing your confidential data. At a minimum, launch the dashboard to see where your starting point is – and then measure the improvement periodically.

Remember that security is never ‘set it and forget it’. You or someone you designate (and trust) should periodically review your Microsoft Secure Score. Technology and services are constantly changing. So will your Secure Score. Release that inner gamer in you and “shoot” for the highest score possible.

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She a co-author of 18 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional and a nationally known expert in the area of digital forensics. He and Sharon provide legal

technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.
jsimek@senseient.com.