How Secure is Office 365? What Lawyers May Not Know

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

© 2018 Sensei Enterprises, Inc.

Can Office 365 "Go Down?"

Oh yes, it can. And it most certainly did on April 6, 2018. The outage was experienced in Europe, notably the U.K. as well as in Japan and other regions of the world. As one British newspaper noted in typical fashion, "Microsoft's Office 365 service is suffering widespread borkage across Europe, again." We do love 'Brit-speak.' Another newspaper said "It would appear that Redmond has opted to secure user data by, er, removing access to it entirely. Clever."

An unhappy customer wrote "Get this sorted – not been able to access account at all and working from home. Losing business here!"

Pete Banham, cyber resilience expert at Mimecast, commented: "Microsoft Office 365 was hit with major downtime on Friday, with customers around the world unable to access their services or admin portals. An operational dependency on the Microsoft environment creates business risks that need be addressed." He went on to say that entities need to consider a cyber resilience strategy to allow them to recover from such an outage.

To Microsoft's credit, it announced later the same day that it had fixed the authentication problem. Certainly, it didn't solve the PR problem emanating from all the users who couldn't login.

That certainly made us wonder how long an American law firm would be able to tolerate an Office 365 outage. This is an unsettling thought to many law firms which never thought about Office 365 being unavailable to them.

Creating a cyber resilience strategy

We could write an entire article for creating a resilience strategy, otherwise known as a business continuity plan. If Office 365 has a problem, how does a firm remain functional with e-mail, preparing documents, etc.? This is the point at which you plan to fail. Our recommendation is to use other services that integrate with Office 365. While there are many alternatives, we'll give a few suggestions to keep you running during an Office 365 outage.

E-mail is now a required service for any law firm. Microsoft has a lot of redundancy for Office 365, but we've already seen some major failures. Consider routing your e-mail flow through a service like Mimecast or Proofpoint. Should Office 365 (or hosted Exchange) go down, you can still receive and send e-mail just like you normally would. Once Microsoft comes back up, the "offline" activity is synchronized with Office 365. You'll need to work with your IT folks to get the configuration right, but it is possible to still operate during an Office 365 failure.

File access is another concern for continuity. You can control which OneDrive files are available offline. Access to the Office software (Word, Excel, etc.) isn't an issue since part of the Office 365 subscription is to have local installs of the software.

Other Office 365 services such as SharePoint may be more difficult to engineer offline access. Most firms will be just fine with e-mail and file access. The good news is the extended failures of Office 365 are very rare.

Are you responsible for securely implementing Office 365? In a nutshell, yes.

Lawyers look at us blankly when we ask, "How secure is your implementation of Office 365?" But it is a question posed by Microsoft itself. Let us offer a small tidbit from Microsoft's "Introducing the Office 365 Secure Score" web page:

"Ever wonder how secure your Office 365 organization really is? Time to stop wondering - the Office 365 Secure Score is here to help. Secure Score analyzes your Office 365 organization's security based on your regular activities and security settings and assigns a score. Think of it as a credit score for security."

Office 365 isn't magically secure out of the gate. It needs some help from your end. Secure Score looks at the Office 365 services you use and then looks at your settlings and activities before assigning you a score that represents the quality of your security practices.

When we get a new client that is using Office 365, it is standard practice now to run "Secure Score." And the results are usually dreadful. You don't have to reach the pinnacle here – as we always say, the object is to "get to good."

While we don't know the exact percentage of law firms using Office 365, we do know that lawyers are flocking to it in ever-increasing numbers, at least in our experience. Our best guess is that 35-50% of law firms are now using Office 365,

with many more planning a migration to Office 365. So making sure Office 365 is secure is a very big problem in the legal sector.

Attacks against Office 365

Microsoft is very much the victim of its own success. As soon as a large portion of the marketplace turned to Office 365, the bad guys went on the attack. There was the infamous “KnockKnock” botnet attack that was designed to target Office 365 system accounts, which tend to have elevated privileges.

Criminals employing ransomware attacks began to target Office 365 as well – and the attackers were both lone wolves and organized criminal gangs. Cerber ransomware targeted Office 365 and flooded users’ mailboxes with an Office document that released malware via macros.

Collaboration tools can be a source of danger. Using Office 365 with SharePoint Online or OneDrive for Business, ransomware can spread across multiple users, systems and shared documents. One point of entry can cause a domino effect, giving attackers quick access to data, e-mail and networks.

Microsoft has duly noted the threats and, in April, unveiled an Attack Simulator for Office 365 Threat Intelligence. This phishing attack simulator builds on the work of Office 365 Threat Intelligence, released in 2017, which allows IT pros to analyze threats in near real-time and to set up custom alerts. Just Google “Office 365 Threat Intelligence” and see what’s possible. The dark side of reading about it is realizing the full extent to which Office 365 is under attack.

More about Secure Score

In light of the torrent of attacks on Microsoft Office 365, Microsoft has provided, through Secure Score, recommendations for its customers to improve the security posture of access to its service, reducing risk at the same time. There is no silver bullet nor does Secure Score give you an absolute measure of how likely you are to have a data breach. But it does help assess the extent to which you have adopted security controls which can help prevent data breaches.

Rather than reacting or responding to security alerts, Secure Score lets you track and plan incremental improvements over a longer period of time.

While some of the changes to Office 365 for improving security occur behind the scenes, like auditing or reviewing reports weekly, others are more time

consuming and noticeable to users when implemented, like enabling Multi-Factor Authentication (MFA) or implementing a Mobile Device Manager (MDM).

Microsoft takes the guess work out of achieving these security-minded goals by providing a checklist of tasks and instructions on how to complete those tasks. Once implemented, the secure score will go up. The default score after just implementing Office 365 is 27 and the highest score you can achieve is 450. Our recommendation is to shoot for a score of 250 or better, which will help to increase the security of your data stored within Office 365 and reduce the potential risk of a data breach occurring.

Microsoft charges $1.40 per user / per month for Multi-Factor Authentication, $6.00 per user / per month for the Mobile Device Manager (MDM) called InTune, and Advanced Threat Protection (ATP) costs $2.00 per user / per month.

These are not major costs for most law firms and initial costs for configuring these security measures is not extreme, perhaps in the 10-15 hour time frame for a small firm.

General Data Protection Regulation

The EU's General Data Protection Regulation become effective on May 25th, to the consternation of many entities, including law firms, which were not prepared for the very strict requirements of the GDPR. And be aware that violations of the GDPR carry hefty fines.

If you have European Union clients, or store or process data of EU residents, it is past time to roll up your sleeves and make sure you are GDPR compliant. New features in Office 365 can help you meet the strict GDPR privacy requirements. While this is a complex subject, Microsoft walks you through the key changes under GDPR and the implications for Office 365 users at https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx.

On the plus side, Office 365 meets requirements specified by ISO 27001, HIPAA BAA and FISMA, users own and retain all rights to the hosted data, users can view a map of where the data resides, and there is limited access by Microsoft database administrators. Microsoft has done a good job with compliance – much harder is fending off the bad guys who want your data.

Final thoughts

Once again, we caution that there is a difference between IT and cybersecurity. A lot of perfectly good IT consultants can get you up and running on Office 365. But can they get you up and running securely? Most law firm managing partners seem unaware of the possible security dangers that come with Office 365. They want to "set it and forget it." It is clear that this worries Microsoft, which has really begun an extensive campaign to wake organizations up to the security risks (and increasing threats) that may come with Office 365.

One wonderful resources provided by Microsoft is an "Office 365 security roadmap: Top Priorities for the first 30 days, 90 days, and beyond." Again, just Google it. This is one of the resources we've found – and a roadmap is exactly what law firms need.

Now that Office 365 has such a big bulls-eye painted on its figurative back, we applaud Microsoft for taking a hard look at security concerns and trying to address them. But this is a dance that requires a dancing partner and those who use Office 365, especially lawyers, have a duty to make sure they are aware of potential security problems and doing their best to beef up their security posture.

Given the dangers that this article has identified, the time for investigation and action is now.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com