5 File Sharing Best Practices to Protect Business Data at Home

After several weeks of lockdown with its necessary work-from-home (WFH) conditions, we've all adapted fairly well to the WFH basics. We can access our company network and apps, post to the blog and gratefully check the status of our paychecks. Perhaps now is the time to check and improve the security of our business data by implementing some file sharing best practices.

1. Establish a Security-first Mindset

With COVID-19 WFH policies, end users regularly conduct business via home computer, laptop or mobile device. As a result, the network perimeter has largely disappeared. Thus, an organization's WFH security posture would be much improved with a security-conscious staff. Everyone should be mindful of information security and operate with sensible, due diligence.

Employees with access to information are often targeted by social engineering attacks. Consequently, a company's staff is most vulnerable to being compromised, often unknowingly and unaware, because they present to cyber criminals an inside source with access to proprietary information.

Information-security awareness programs and mandatory training must be implemented across the organization. It is vitally important to review and update these programs to reflect WFH conditions and today's threats (like COVID-19 Phishing Scams) to elevate employee awareness. Layered defense and a knowledgeable staff will reduce the risk of a security breach from unauthorized file sharing.

2. Use Business-Grade File Sharing Solutions

Businesses most frequently use email to communicate, collaborate and share documents, images and files. However, constraints in common email services such as file size limits often force users to find other solutions to share information.

Frequently they opt for consumer-grade file sharing solutions to circumvent the limitations. However, these consumer services fall short when it comes to protecting business data. Compliance and eDiscovery issues as well as loss of sensitive data are the inevitable result.

Instead, find a business-grade file sharing service, such as Microsoft 365 (or Office 365), that provides adequate visibility and security. Look for compliance and e-discovery features, flexible access control and other features that prevent data leaks and unauthorized access.

3. Configure File Sharing Solutions Properly

Even business-grade file sharing solutions must be configured properly to provide the data protection you need. For example, Microsoft 365 apps like Outlook, OneDrive, Teams, and Yammer all include built-in features that enable users to more securely share files and be productive. A few simple things you can do to increase file-sharing security include:

- Add permissions to recipients in OneDrive for Business or SharePoint before sending files in Outlook.
- Use password protection to ensure documents are viewed only by authorized parties.
- Send a sensitive message to external users securely by encrypting the message with Microsoft 365 Message Encryption.
- Set password policies and manage security settings in Yammer.

- Configure Azure AD conditional access policies to secure the data in Teams.

Additional options to classify information and share documents securely via third-party applications are found in Microsoft Cloud App Security. You can prevent data loss on mobile devices with Intune and through mobile device management. App-level controls also help to prevent data loss.

4. Invest in Mobile Device Management

The downloading and storage of business data on personal mobile devices creates major headaches for IT security professionals. Fortunately, a host of mobile device management (MDM) solutions can help your organization get control of mobile security.

Choose an MDM system that allows you to specify which devices can access the network, as well as what applications and data they can access. Then use the MDM to:

- Limit access by role or department – "One size fits all" has no place in mobile access. Limit access to only those applications and data needed for users to do their jobs.
- Allow access only to devices with a secure OS – Apple, Android and other providers continually update their security protocols. Allow access only to those devices that have installed recent updates.
- Remote lock and wipe – Enable remote lock and wipe for all mobile devices used for business purposes. This allows you to protect sensitive data from compromise through a lost or stolen device.

MDM solutions like Intune from Microsoft can manage not only mobile devices but also personal home workstations. This ties into its primary function of securing files by providing adequate malware/security protection on endpoints outside the network.

5. Implement a Unified Workspace Solution

A comprehensive unified workspace solution simplifies WFH file and app sharing without disrupting the way companies currently run their IT. Messaging Architects' solution is based on Microsoft Azure cloud technology and the browser-based unified workspace solution from Awingu.

The offering enables and simplifies WFH security by aggregating all company files and applications to one secure online workspace that can be accessed from any device, OS or browser. Businesses are empowered to mobilize all company applications without making changes to existing software or backend infrastructure.

The unified workspace solution offers an intuitive user interface, a mobile app for tablets and administration tools. No plug-in is required on the end-user device for hassle-free collaboration. No data footprint is left, and all confidential files remain safe and secure on premise or in the cloud.

File Sharing for Today's WFH Crisis and Beyond

We are saddened by the depth of the current crisis and express our support to those impacted physically and economically. When this is over, new challenges will inevitably arise, be it natural disasters or an international workforce that requires WFH technology and secure file sharing.

Look to Messaging Architects for information governance best practices, Office 365 migration, strengthened WFH security, and cyber defense measures to protect against COVID-19 email threats. From eDiscovery to cloud security and more, we have the tools and expertise to get you through.