Secure File Sharing:

When You Need an Armoured Truck, Not a Courier

Some Files and Information Need Much Greater Protection When They Are Shared

For the last decade, organisations have made substantial efforts to identify and protect their most sensitive and confidential information when it is stored in their digital infrastructure. To secure this critical information, firms have implemented m ore stringent access, stronger encryption, more layers of security and new types of infrastructure. Generally, all information held by these organisations is protected in these ways — when it is at rest. But things can break down when the information is in transit, as when it is being shared. Highly confidential data and critical digital assets should always be well protected in transit, but the sharing of less sensitive (but still valuable) information isn't as closely scrutinised. The result is something like using an armoured truck to protect large shipments of cash or securities, while using a bicycle courier to convey small amounts of money or less sensitive assets.

Diligent

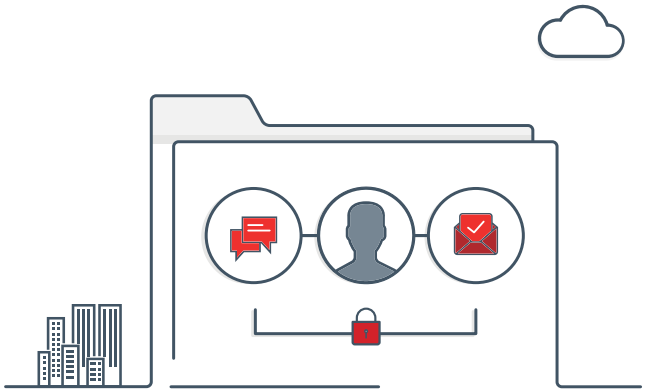
In this analogy, the bicycle courier can represent file-sharing tools such as Box or SharePoint or unencrypted email. They cannot be relied upon to prevent data from being lost or stolen. In fact, with many standard file-sharing tools, it is impossible to know whether data theft has occurred. This is because most of them were never designed to be ultra-secure, but instead were created with ease of use as the priority. But with data breaches becoming a daily fact of life at organisations of all sizes, and with regulatory compliance looming ever larger in corporate governance, upgrading from that virtual bicycle courier to a virtual armoured truck is essential.

The reason for this is that the corporate risk from semi-secure file sharing is greater than most firms realise. Standard Enterprise File Synchronisation and Sharing (EFSS) solutions simply lack sufficient controls to prevent unauthorised storage and forwarding of sensitive data. And the use of the regular corporate networks for sending these files opens them up to hackers that are most likely lying in wait to steal valuable information. The chance that cyber-attackers have penetrated a network and are lurking without the knowledge of the organisation is astonishingly high. Infocyte's research has found that the average "dwell time" for malware inside an organisation's systems can be as long as 800 days before it is discovered.

There are other drivers for implementing a purpose-built secure file-sharing platform. The most obvious is to meet compliance demands. Without strong controls for data sharing, it is impossible to meet many specific compliance regimes. And with the deployment and use of a secure file-sharing system, it is much simpler to prove compliance. In addition, proactively providing key employees or teams with a more secure method of file sharing helps stop activities that put information at risk.

Deploying an ultra-secure file-sharing system is a natural extension of the effort to protect sensitive, private or valuable information. Security and compliance teams know that data must be protected both at rest and in transit. Secure file-sharing solutions provide essential protection for the most common in-transit scenario.

The Use Cases: When the File-Sharing Armoured Truck Is the Right Solution



The move to all-digital information is happening quickly. Even in industries in which paper documents are the norm, digital versions of them are common. And with digital information, the potential for loss, theft or other risk to the data increases substantially as files fly around the organisation. Risk management teams are now realising that there are many organisational business processes that rely on sharing confidential information and they need a more secure method for doing so.

Focusing on the many use cases in which a fully secure file-sharing system is necessary helps provide an accurate scope of the problem. The following list provides examples of common business processes or use cases where highly secure file sharing should be used:

- **Director and board activities.** This may be the most obvious use case. The level of secrecy and confidentiality necessary to protect files shared among board members and senior management is obvious. Cyber-attackers know this and are often focused on the high-value information communicated by these individuals. They may be monitoring less secure EFSS tools to enhance their chances of intercepting it.
- **Product design and development.** As the theft of intellectual property (IP) and technology development information continues to increase, many data thefts occur when files are shared, but not protected. Employees may download files to personal devices, creating an unsecured copy. And partnering is common, so contractors and external firms may get copies of key files as well. Without secure file sharing, product development files can go almost anywhere.

- **Audits and auditing.** During an audit, unfettered access to information and data files is common. Accidental loss of files may occur, particularly if there are insufficient controls on these files as they are shared with auditors.

- **M&A or financial engineering activities**. This is also a somewhat obvious use case that would commonly use highly confidential information and require sharing files that would have substantial negative impact were they to become available to unintended recipients. A secure file-sharing solution that provides a "secure data room" would also help to ensure that restricted information stays that way.

- **Intellectual property (IP)**. IP theft has become a common problem and a major focus of financially focused cyber-attackers. In addition, theft of IP by trusted staff is increasing as well. For this reason, a secure file-sharing platform has become an important component of protecting IP and ensuring it is not stolen.

- **Sensitive human resources (HR) files.** Although not as valuable as new product plans or the details of a corporate acquisition, the embarrassment and impact of leaked HR files and payroll information can be substantial. The disruption can impact the organisation for months. This is a more common problem than is typically thought. For example, Facebook payroll data on 29,000 employees was recently breached.
- **Sensitive executive-level communications.** There are often instances in which executives are communicating information that must not be seen by anyone else. It could be a legal issue, a personnel issue or a product problem. Ensuring that no one – not even IT administrators – can see these messages is essential to keeping them private and secure.

- **Litigation/legal information.** There are many files and datasets that either support or document legal actions or litigation. In some cases, these files are required to be kept confidential. In other scenarios, governance or legal standards require that these files be highly protected. In many legal departments, the weak link in protection is when files are sent to others that need to review them. For this reason, secure file transfer is a necessity for internal legal departments or outside counsel.

- **Crisis management.** Managing a crisis is difficult enough without information leaks that can scuttle the crisis management strategy. Crisis management often requires using outside teams that need confidential information. Ensuring that this data is protected and secured, not only during the crisis but afterwards, is non-negotiable. Implementing a secure file-sharing platform prior to a crisis ensures it can be used immediately if a crisis occurs.

- **Corporate restructuring.** Staffing changes require a highly coordinated and confidential plan of action. Yet there are also many individual contributors to the plans for these restructurings that need critical information. The result is that confidential files are being sent to many places in the organisation. Letting this sensitive information sit in less secure EFSS is asking for trouble and pre-disclosure.

- **Board committees.** To support the activities of the board, many organisations create standing or ad hoc committees that focus on key operational aspects of the organisation. With the strong linkage to the board, the use of confidential files and information is common. Yet many of these committees use their everyday EFSS tools. Given that many of the files that are shared by these committees need to be strongly secured, using a secure file-sharing system for board committee work should be mandated.

There is another mega-trend that results in sensitive files being shared in unsecured ways. This is the broad utilisation of analytics that depends on key corporate datasets and files. Most of the input data for analytics is not sensitive, confidential or in need of a high degree of protection. However, in an increasing number of instances, sensitive files are being used. Unfortunately, most analysts are focused on the outcomes, not on protecting underlying data files. Deploying a secure file-sharing platform now to protect confidential data used for analytics in the future will make it easier to protect confidential information.

**SECURE FILE SHARING &
SECURE MEETING WORKFLOW**

Diligent Provides a Proven Solution for Secure File Sharing

To meet the need for more secure and protected file sharing, Diligent is offering a best-in-class solution. The offering can support the many different use cases, providing broad value to the organisation. The design point for this product is fundamentally different from common EFSS services. It starts with Diligent's decision to create a secure file-sharing p latform t hat s tarts with a focus on security, rather than adding it on. One example of this: Diligent Secure File Sharing is not run on the general corporate network. The solution is deployed "off-network" in a closed secure environment. Instead, Diligent provides a secure, closed environment. This eliminates many threats and prevents cyber-attackers from using access to the corporate network to steal sensitive or confidential files. Diligent enjoys an unparalleled reputation for security and information protection from its years of supporting the work of boards of directors. In addition, Diligent offers secure integrated workflow capability. Most, if not all, EFSS solutions don't have this. As a result, sensitive information can be compromised during the collection and distribution of this information.

By focusing on security first, Diligent eliminates many common vulnerabilities that exist when sending confidential information with an EFSS. To start, this solution has IT shielding, preventing IT teams from having access to files. In contrast, EFSS systems generally allow IT administrators visibility into any files within those systems. There is also secure, traceable document delivery. This provides an audit trail of who has the information, when it was viewed and other details about any secure file sent to other individuals. The Diligent Secure File Sharing solution allows files to be restricted from being either forwarded or downloaded. This functionality is essential to preventing sensitive files from being sent to places that they shouldn't be. There is also dynamic watermarking that provides clear audit trails and a greater degree of document control and protection.

Diligent Secure File Sharing is also a good team player. It is designed to augment and work with less secure EFSS products. Employees now have access to both the armoured truck and the courier without a lot of complication and complexity.

KEY TAKEAWAYS

Nearly every organisation has dramatically improved its ability to secure and control confidential information when it is being stored. However, when these sensitive files are being shared or communicated, protection is often lacking. Many common business activities that utilise confidential files need a secure file-sharing platform. Deploying a secure file-sharing system now allows an organisation to start limiting its risk immediately. Once files are disseminated in an unsecured manner, it is often only a matter of time before they end up in the wrong hands. A secure file-sharing system ensures that this does not happen.

Employees need a range of security options for file sharing. The semi-secure EFSS solutions are already in common use. Now businesses need to add a highly secured and controlled file-sharing platform for confidential information. In much the same way that a physical asset can be moved using an unsecured courier or a highly secure armoured truck, digital information sharing must be supported with a range of file-sharing solutions, each delivering appropriate security. Diligent is a leader in secure business activities, known for reducing risk, meeting compliance demands, and protecting communications at the senior executive and board level. This expertise is the foundation for delivering an optimal solution for secure file sharing. For more information on this secure file-sharing solution, please go to:

SECURE FILE SHARING & SECURE MEETING WORKFLOW

SAFE AND SECURE COMMUNICATIONS

Download on the App Store | Get it from Microsoft | GET IT ON Google Play | AICPA SOC | ISO 27001 CERTIFIED BY BRIGHTLINE

"Diligent" is a trademark of Diligent Corporation, registered in the US Patent and Trademark Office. "Diligent Boards," "Diligent D&O," "Diligent Evaluations," "Diligent Messenger," and the Diligent logo are trademarks of Diligent Corporation. All third-party trademarks are the property of their respective owners. ©2020 Diligent Corporation. All rights reserved.

To learn more about Secure File Sharing by Diligent, contact us today:

Call: 1800 646 207
Email: info@diligent.com
Visit: www.diligent.com