

Your Documents Aren't Safe. Here Are the Best Practices for Document Security

Opinions expressed by *Entrepreneur* contributors are their own.

With the advent of 5G technology and Industry 4.0 putting more pressure on businesses to fast-track their digital transformations, the demand for document-management solutions has exploded. The worldwide market for document-management software is projected to reach \$10.17 billion by 2025. Along with this revolution comes inherent concerns about properly securing all this information. Documents often contain sensitive and private information that, if compromised, could be detrimental to individuals, businesses or governments. That is why companies need to incorporate the highest levels of document-management security.

Related: [Keep Your Information Moving At The Speed Of Your Business](#)

Don't wait to secure digital documents

With the continued release of new vulnerabilities regularly and the ease at which a digital document can be compromised – compared to a physical piece of paper – ensuring the security of those documents has become more important than ever to keep private information from being exposed.

It is common to read the news and learn about a new security breach. Impacting small and large companies, nearly 2000 data

breaches occurred in the first half of 2022 alone. To many companies, their data is among their most valuable assets, so it must be protected.

Ransomware, a form of malware designed to encrypt files and deny users access to them until a demand ransom is paid, is one clear threat. Phishing attacks, where hackers try to get account credentials (username and password), represent an ongoing and ever-evolving danger. Hackers typically lay low for a time, then eventually start logging in as that user so as not to draw suspicions. Then they download documents that the user can access or, if sophisticated enough, attack network administrator privileges.

Just who is trying to hack into systems to get documents? Anyone who can find value in the type of data a company possesses. Hackers typically don't know the type of data a company possesses until they get their hands on corporate documents or know enough about a company to recognize the types of information that might be available, such as financials or employee personally identifiable information (PII). It's really any documents that they can use for profit.

What to look for in a document-management partner

Numerous outsourced document-management vendors exist in the marketplace today, and not all are created equal when it comes to offering the highest levels of security. Below are four necessary security features to look for from a document-management partner:

1. **End-to-end chain of custody and tracking:** It's important to know who has had access to both physical and digital documents. Chain of custody is crucial throughout a document's life cycle. Any access should be logged so that you can see who opened a particular document, when

and what their reason was. Partners should be able to show audit and chain-of-custody logs. This also helps ensure that only people with the proper privileges can access particular documents – and no one else.

2. **Disaster recovery, failover, redundancy, and guaranteed access:** With a reduction in paper documents, systems and processes need to be in place to ensure that your digital documents are accessible in the event of a single point of failure. At the partner's data center, if the internet goes down, you still should have a backup, redundant way to access those docs. Partners should be able to provide written reports that show testing on an ongoing basis along with results, so you feel confident that if disaster strikes, you know the failover will work properly.
3. **Compliance with industry standards:** Compliance standards, such as PCI for credit card information, HIPAA for health information and SOC 2 Type II for policies and processes, ensure complete accountability for the security and related processes around any document. Compliance usually involves an independent third-party assessment to ensure that partners are following industry guidelines, performing the necessary tasks and have the appropriate controls in place to ensure the highest levels of security. Partners should be able to provide evidence of certifications, indicating they meet the necessary compliance standards for the types of documents that you're storing.
4. **Utilization of a "continuous ongoing compliance" model:** One of the drawbacks of compliance is that it's an annual assessment, so sometimes companies get lax throughout the year – then get ready just at compliance time. Partners should be able to demonstrate compliance not only at assessment time but also throughout the year.

Related: [How To Develop Security Policy For Your Company](#)

Best practices companies can implement

In addition to wanting the best technology solutions to help facilitate the digitization of documents, companies should also make security a top priority. Whether you have a Chief Security Officer, Chief Technology Officer, Head of IT or are working with a third-party service provider, there are several best practices that companies themselves should implement to ensure they're doing their part to secure their digital documents:

- Make security a primary, proactive focus and not an afterthought;
- Perform a complete audit of all access to and actions taken on each digital document;
- Ensure proper data classification, retention, and destruction protocols are established and followed;
- Test and document disaster-recovery and business-continuity solutions;
- Run regular vulnerability scans of the environment and remediation of all critical vulnerabilities found;
- Hold recurring security-awareness training with 100% required staff participation; and
- Conduct regular chain-of-custody and security audits to ensure best practices are being followed and documented.

To obtain the highest levels of security for digital documents, collaboration on strategy should involve all stakeholders – including document-management providers, IT, security and operations.

<https://www.entrepreneur.com/article/437661>