The Hard Lessons of COVID-19 for IT Organizations

Remote, Distributed Workforces are the "New Normal"

The COVID-19 pandemic has proven to be disruptive in more ways than epidemiologists could have imagined. Aside from insights into some of the shortcomings of our global health infrastructure, the crisis highlights other weak points in systems and processes that support our workplaces.

While globalization has driven increased levels of interdependency between organizations around the world, what has lagged is the ability of organizations to support fully virtual organizations comprised of at-home workers.

The underlying technology to support this model has been in place for decades – however, resistance to change has stunted progress in this area for most sectors outside of high tech.

How Do Organizations Adapt?

IT organizations have typically supported remote workers using a variety of hardware and software tools that only imperfectly address the needs of a more fully distributed workforce. To serve a broader community of workers as necessitated by events like COVID-19, extending these tools and practices in new ways is required.
Some of these adaptations include:

Put an end to the practice of local file storage

For many workers, storing files locally to perform their work has for decades been the norm. Locally edited files are further shared via email, groupware, or applications to facilitate a work process. In this working model, the local copy of the file is retained…often to the detriment of the organization's information security. Laptops can be hacked, stolen, and compromised in ways that make this local cache of files a huge liability that can expose customer or employee data. In today's world of ubiquitous connectivity, there is no compelling need for local file storage for most workers. Implementing policies to limit access to local file stores and instead leveraging online, centrally-managed, secure alternatives by default is essential.

Author on-line by default

·Content creation has traditionally been facilitated through local applications. In recent years, however, tools like Google Docs, Adobe Creative Cloud, and O365 have provided a more secure cloud-based alternative to traditional authoring tools. Leveraging cloud-based tools like these for all content creation helps to ensure that potentially sensitive data is not only stored in secure, centrally-managed locations but that is "born" there – helping to improve the security and integrity of that data even for the most distributed workforce models. For this reason, online authoring should (for most organizations) be the default work mode, with the sole exceptions being those associates who may travel and thus at times be without connectivity.

Implement, train, and enforce good InfoGov practices

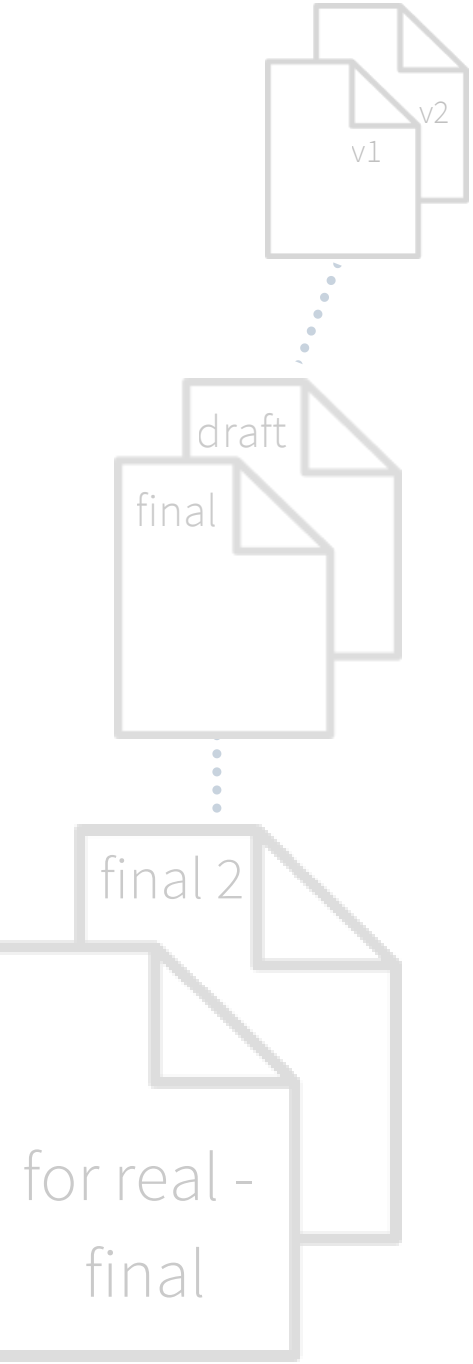
For most organizations, the changes outlined so far can be relatively easy and organic ones, since most IT teams are rolling out these tools anyway. The challenge will largely be around user training and process enforcement, which leads us to the next points, which are arguably the most challenging.

Links, not attachments

Collaborating via tools like email and instant messenger often involves sharing files, not just text. Too often, this is done by attaching new instances of the file – both within the tool itself, as well as on the file system of the recipient who opts to save it off. In the type of environment needed for efficient, secure distributed workforces this kind of practice creates an unacceptable risk of data loss. Instead, associates should be trained to leverage links to a single, authoritative version of the document in place of disseminating attachments. Doing so has a tremendous positive impact on information governance, data integrity, associate efficiency, and IT cost.

Hardcopy no more

Commentators have long predicted the dawning of the "paperless workplace" only to see hardcopy live on despite its inherently poor level of security and high cost. At one time, the continued use of paper was tolerated because of technical or ergonomic limitations of digital alternatives – display screens were too small or lacked sufficient resolution, mechanisms for digital signature were immature, etc. Today, most of these limitations are a thing of the past and the vast majority of use cases for paper-based work are no longer applicable. Eliminating the reliance on print for almost all use cases is now a practical possibility, and should be enforced.



Native versioning, not new file instances

One of the lingering bad habits of many workers retained from legacy file servers is the tendency to create multiple instances of a file as a primitive, ad hoc form of versioning. How many of us have searched for a document only to find multiple instances – version 1, version 2, FINAL, FINAL v2, FINAL FINAL FOR SURE, and so on? When file-sharing tools had little or no native versioning capability, this practice had some rationale – it helped preserve work during the collaborative process that might need to be resurrected.

However, today's authoring environments like Google Docs, Office 365, and Creative Cloud incorporate versioning as a native feature. This means that the platform transparently maintains a history of all document versions, allowing authorized users to access these deprecated versions or even perform a rollback if needed. While this capability has been present for some time, many users (particularly those who came into the workforce in the days of "dumb" file servers) need training to enforce better behaviors and help ensure optimum data privacy protection and integrity.

Disable screen capture

Many of us rely on screen capture to share what we're seeing on-screen with other users either for collaboration or to debug issues. The technology behind screen capture is admittedly convenient and easy to use. Unfortunately, it also carries significant risk when users inadvertently perform screen captures of applications housing sensitive employee or customer data. Using either Windows configuration options or third-party applications, IT can disable screen capture functionality to eliminate this potential source of data leakage.

Enforcing These Best Practices Over the Long-Run

The recommendations outlined in this article likely make good sense to readers and can be addressed through a concerted initiative given the impetus provided by COVID-19 and its aftermath. Visibility for these issues is currently high, and engagement by affected stakeholders is relatively easy to secure. However, when the emergency is months or years behind us, how do we maintain the momentum and ensure that the measures outlined in this article are sustained over the long-run?

Perform regular discovery to ensure best practice compliance

Investing in solutions like .discover is a critical component to ongoing compliance with remote workforce information management best practices. By connecting to the places where enterprise information accumulates – namely premise and cloud-based file shares, email applications, groupware platforms, and instant messaging tools – records specialists, IT, and legal teams can help monitor compliance and provide corrective feedback as needed when bad practices resurface.

Leverage content automation tools to better categorize information

The improvements to the information landscape outlined in this piece can be further enhanced by using the discovery tool to augment and enhance information metadata to make it more discoverable and usable. Content automation solutions like .process can help with this and can automate content categorization and metadata enhancement based on defined rules, machine learning via training "examples", and where needed the engagement of human reviewers. Content automation enhanced with machine learning is an essential part of ongoing information maintenance since the volume and diversity of enterprise information being governed exceeds what can be managed by manual processes.

Define and enforce policies to better govern the information lifecycle

Even when best practices for remote workforce information management are in place and working effectively, it's critical to manage that information coherently and consistently to ensure better compliance with internal, industry, and regulatory requirements. The effort outlined in this article is an excellent catalyst for applying a more global policy management capability to enterprise information to ensure that information managed outside the context of formal records – including email correspondence and instant message communications – are retained and disposed of in ways that are consistent, transparent, and defensible.

By utilizing innovative tools and processes, records management, legal, IT and compliance teams can help ensure that the enhancements to the information ecosystem made to support the remote workforce in the wake of the COVID-19 crisis are sustained over the long-term in ways that benefit users and the organization as a whole.

The Benefits of a More Concerted Approach to Distributed Workforce InfoGov

Many of the initiatives and ideas outlined in this article are ones already in play in the weeks and months before the COVID-19 epidemic. The benefits were in many cases well-understood, if not at that time perceived to be critical to business continuity. Today, the profile of this type of investment in resources has risen dramatically, and these efforts will only accelerate.

The recommendations outlined in this article carry a degree of cost – both in terms of IT governance, as well as in end-user training and best practices. However, the cost is small relative to other IT cost centers and carries substantial operational benefits that include:

Greater workforce flexibility

Having the ability to allow workers to do their jobs from home has substantial benefits in terms of continuity of operations. It also allows organizations to better leverage resources with scarce skillsets during times where personal matters that require them to be away from the office – for instance, while caring for a family member, recovering from a surgery or illness, and so on. Allowing workers the flexibility to do their jobs from any location means those workers can be utilized efficiently when personal or logistical constraints like COVID-10 emerge.

Lower facilities cost

Allowing workers to do their jobs from home over the long-term (not just as part of a crisis) means that outlays for office space, furnishings, utilities, etc. can be reduced over time. For most organizations these costs are substantial, and the savings can be redirected toward more cost-efficient operations, or into innovation.

Lower IT costs

Often forgotten in an age of relatively cheap storage, the vast proliferation of duplicate files has a massive impact on IT budgets. Reducing the volume of information "bloat" (which may account for up to 85% of stored data according to[1] backup data services provider Veritas), IT organizations can reduce unnecessary expenditures and focus their investments in more productive areas.

1: https://www.veritas.com/news-releases/2016-03-15-veritas-global-databerg-report-finds-85-percent-of-stored-data

Lower risk profile for data breach / data privacy loss

Whether supporting workers at home or in a centralized traditional office environment, these recommendations will lead to a more secure information environment. Reducing the proliferation of duplicate files, leveraging secure cloud-based platforms, eliminating reliance on hardcopy, and tightening OS gaps like screen capture combine to create an enterprise IT landscape that reduces the risk of a data privacy incident or breach.

Enhanced productivity

Reducing the volume of information clutter, sharing single versions of authoritative, approved content, and utilizing more effective native document versioning features are all good ways to create a more productive, informed workforce. Studies by organizations like McKinsey have shown that workers in many organizations spend up to 35% of their working time simply finding the content to do their jobs.[2] Reducing the volume of extraneous content and making it easier to find approved, current versions of policies and procedures has the potential to dramatically reduce this number.

2: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-social-economy

Adopting Change

COVID-19 has made it evident that during events like a global pandemic – no longer the stuff of dystopian science fiction, but a recurring reality given the growth in worldwide populations and travel volume – organizations must find ways to support efficient operation using remote, work-from-home resources. Further, they must do so in ways that employ good Information Governance practices to ensure that distributed operations do not bring unacceptable costs in terms of data privacy protection.

The time is now for both commercial and public sector organizations to adopt these and other changes to empower their workers to work productively and securely from home. Doing so will have cost and efficiency benefits, and will better prepare us all for the unforeseen challenges that the future will bring.

About Us

The team at Nyxeia is composed of some of the world's most experienced experts in all aspects of Information Lifecycle Management. Our team of experts have worked in diverse technology areas including records management, enterprise content management, archiving, digital asset management, document management and leverage this heritage to help deliver the world's most innovative Information Governance solutions.

Contact Nyxeia to learn more about how our skills can help your organization meet its most critical information governance challenges!

nyxeia
Insight Reimagined™

info@nyxeia.com
1251 Avenue of the Americas, Suite 3F
New York, NY 10020
+1 (303) 854-9890