

# EMAIL

## Challenges and Perspectives for the Future of Work



White Paper

“There will be more than **3.8 billion** email users before the start of 2019.”

- Radicati Group (2018)

### Historical Background

Email as we know it has its genesis back to the 1960's and 1970's where it's peer-to-peer level of communications fueled communication systems development towards what we now know as the Internet. A sponsored 2010 study on workplace communication found 83% of U.S. knowledge workers felt email was critical to their success and productivity at work (O. Malik, GigaOm "Is Email a Curse or a Boon?"). With billions of emails in use today and many of those applicable to the enterprises of tomorrow, it's helpful to explore the benefits and risks of email in the context of its future application for corporations.

**83%** of U.S. knowledge workers felt email was critical to their success and productivity at work, in 2010.

-O. Malik, GigaOm "Is Email a Curse or a Boon?"

### Exceeding an Intended Use Case

The use of email has been profound for organizations. Every public and private enterprise in the world including government agencies leverage email as a system of record and as a prime communication tool for employee engagement and for critical communication-based interactions with customers, suppliers and partners. As such, email has exceeded an intended focus on 'messaging' and has now placed itself in the center of organizational information technology and content. While noble in aim, the resulting impact of wide-spread use of email as a predominant communication platform has far exceeded its intended purpose and the demands upon it have outpaced its ability to fully serve the security and content-based collaboration needs of its users.

**Canon**

CANON INFORMATION & IMAGING SOLUTIONS

## Critical Challenges and Risks

Email is a key threat vector for enterprises (Barracuda – 2018). With phishing and other attachment-laden threats, email poses one of the most severe security risks for organizations.



The predominant issue with today's use of email is that it unfortunately houses some of an organization's most critical enterprise content and intellectual property. Email was never designed to be a formal system of record and with the advent of 'attachment' handling capabilities, email as a solution continues to serve as a poor mechanism in the critical content management space. File size limitations, inefficient storage utilization, high infrastructure demands, provisioning/deprovisioning challenges, intensified regulatory environments (GDPR, HIPAA, etc.), and security risks are some of the key challenges organizations face when placing email at the center of information technology content management and collaboration strategies. By some estimates, about 40% of vital enterprise-level content is stored and acted upon via email.

Let's now explore some of these key challenges with today's use of email:

### Security Risks:

Email is a key threat vector for enterprises (Barracuda – 2018). With phishing and other attachment-laden threats, email poses one of the most severe security risks for organizations. Security, as such, is multi-faceted.

First, most organizations rely on end-users to use foresight and constraint with regard to email and email attachment handling. An organization may have a policy that restricts intellectual property from being released via email attachment to outside vendors for example. However, with one missed key stroke, a well-intended employee can accidentally release sensitive email communication or email-based attachments to an outside party without realizing it. Thus, user-level security rarely succeeds, and this is often not due to malice on the part of the end user.

**40%** of vital enterprise-level content is stored and acted upon via email.

In a recent study, 41% of workers admitted to deliberately bypassing security policies. 57% of these employees stated that this was because it was the most efficient way to get things done. (Forrester, "Evolving Security To Accommodate The Modern Worker"). As we've seen from some of the most publicly visible breaches of late, external threats to organizations specific to email are real. A threat vector such as email can allow a gateway for hackers and ill-willed individuals to hack into an organization's email (normally via phishing scams and email attachment based viruses) and once inside, access critical organizational content. This threat places at risk not only the affected organization, but also any external constituents who may have shared content with it.. Shadow IT and other employee-level work-arounds also pose a severe risk for the enterprises of tomorrow.

Email security threats extend beyond bad actors and includes events that compromise data security without malicious intent. These events may involve content mishandled by users in the form of accidental deletion of important messages, or software failures such as corrupted Outlook databases and PST files. Furthermore, even when email is preserved, email accounts are often hard to search for rendering content essentially lost. Examples include employees who are on holiday or who have left an organization. Their email-based content is difficult to access for the organization and may pose a latent security threat.

As such, email-based security remains a viable threat to the enterprises of tomorrow.

### **Workflow and Collaboration Challenges:**

With much of an organization's communication occurring via email, challenges surface and create a drag on organizational efficiency. Workflow is impeded via legacy use of email and email attachments. Problems with email content version control and file size (including file-type issues forcing use of expensive end-user software), all raise their head to create challenges for organizations. Collaboration via email is also a daunting task and fails to achieve its intended purpose. Email works fine as with messaging applications where point communication ensues. However, once organizations attempt at-scale collaboration and workflow automation, especially given the emergence of unstructured data-driven artificial intelligence and machine learning, email becomes a serious drag on an organization and may surface end-user dissatisfaction with the conduct of work..

**41% of workers admitted to deliberately bypassing security policies.**

**57% of these employees stated that this was because it was the most efficient way to get things done.**

-Forrester, "Evolving Security To Accommodate The Modern Worker"



Per a 2018 Dell EMC report, "43% of workers send work related emails from their personal accounts, with some 71% of employees needing to share files with third-parties daily or weekly." As such, security-focused 'collaboration' including content resident in today's email systems is key when considering digital strategies for the enterprises of tomorrow.

### **Integration Challenges:**

A predominant challenge with today's use of email is its failure to fully integrate into the systemic workflow of an organization. If 'some' client communication is handled via social platforms (e.g. Chatter provided by Salesforce), other communications are via social network feeds such as Twitter, Facebook Workplace, LinkedIn, Slack and other collaboration platforms, adding email threads into the mix creates a significant challenge for organizations. This multi-threaded mechanism fails to live up to the expectations of the typical organization and certainly fails to meet the ease of use aims and content collaboration needs of the enterprise when dealing with suppliers, partners and the customer eco-system. Email as a stand-alone communication platform typically isn't integrated well into the larger enterprise IT ecosystem, and it remains a constant source of risk to the system.

**43% of workers send work related emails from their personal accounts, with some 71% of employees needing to share files with third-parties daily or weekly."**

-2018 Dell EMC Report

**The average employee spends 28% of his/her work week just reading and responding to email. Other studies have identified frustration with email as a top complaint. This is why we're seeing a growing field of entrepreneurial companies that are radically rethinking email and how we communicate online."**

-McKinsey Global Initiative

## **Perspective for the Future of Work**

With a forward vision towards the Future of Work, a few observations are critical to consider. With approximately half of the planet relying on email-based communication, we will not see in the shortrun a full and outright displacement of email as a communication tool. The challenge for organizations therefore resides in its ability to:

- improve collaboration;
- improve organizational workflows;
- improve employee engagement;
- include email and email attachments into core Cloud Content Management strategies;
- place limits on costly IT overhead and;
- proactively address viable security threats inherent to the use of legacy email applications.

**"Email reflects the communication expectations of past generations, and isn't the tool of choice for the millennial generation, who have grown up texting and using social media."**

-Entrepreneur Magazine

In order to achieve these aims, Canon Information and Imaging Solutions (CIIS) as a leading provider of digital content solutions believes we are at the cusp of re-imagining email as we move through the 4th Industrial Revolution and envision the Future of Work. As social and collaboration platforms continue to make their mark on the organizations of tomorrow, the key challenge is how to address and minimize the email-based threat surface that organizations experience and how to reimagine email such that it is leaner, more efficient, and can interact with IT boundary systems in a more complimentary manner. A key component in achieving these objectives is simply to 'get content out of email'. With some 40% of organizational content residing in the email paradigm, it is also vital to address the security threat vector. Furthermore, if content and attachments can be moved automatically away from email's threat vector and into secure cloud content management platforms that were built specifically for secure and collaborative content management (e.g. BOX.COM), organizations can immediately reduce their threat surface with respect to breach events all while expanding the collaboration potential around that same valuable enterprise content.

In partnership with Canon, emerging companies such as San Francisco's mxHero ([www.mxhero.com](http://www.mxhero.com)) have built novel solutions which automatically capture inbound and outbound email attachments and place those content attachments directly into secure collaboration platforms such as Box. In so doing, a number of goals are achieved. First, these solutions do not require end-user intervention. With user-adoption being a key driver for new Software as a Service (SaaS) based solutions, this is critical. If end-users can use email exactly the way they do today, point solutions such as mxHero's Mail2Cloud platform can automatically detect and extract key email-borne content attachments and automatically uplift them into targeted cloud collaboration platforms. Secure links are then re-inserted into the email flow allowing secure, collaborative access to that very same content while reducing collaboration overhead and security threat surfaces for the enterprises of tomorrow.

Companies that deploy such email solutions gain a number of additional advantages. Auto-addition of critical metadata tagging enables content searchability. Governance and retention policies around that content can be automatically applied, and once the content is automatically placed into the content management platform, integrations with other boundary platforms will ensure access to the right content, at the right time, for the right user. As stated by Fast Company "mxHERO is like Mission Impossible for email." With the emergence of enterprise-wide content management strategies, we will also see a future where AI and Machine Learning will be applied to core content within the enterprise to drive workplace collaboration, digital business strategies and security aims. Excluding email-based content from this innovation will impede the future of work. Email in today's form, is simply ill-equipped to handle this on its own.

**"The Future of Work will require edge innovation including content centric strategies for Machine Learning and Artificial Intelligence. Unstructured data and email-based content will be core considerations as the enterprises of tomorrow formulate strategies to drive digital innovation.."**

-Dennis Amorosano, SVP and GM, Canon Information & Imaging Solutions

**"70-80% of enterprise software isn't equipped for the modern workplace culture."**

-Aaron Levie, CEO, Box

## Summary

Digital transformation is being undertaken at a rapid pace across enterprises in all industry sectors. Content is a relevant and horizontally applicable consideration for the organizations, and each of them will have its own unique set of challenges to address. Law firms and legal business units will want to take advantage of these innovations while ensuring compliance, security and client-attorney privilege remains intact. Healthcare providers and Life Sciences firms will want the same solutions while ensuring compliance against regulatory aims such as HIPAA, PHI protections and GxP validations. European GDPR requirements will be a key consideration especially for multi-national firms. Marketing organizations will increasingly seek solutions built around their ability to drive creative content strategies and collaboration. All industry sectors including government and education will benefit from innovations in the market aimed at solving critical user-level challenges with the use of technology; especially where those targeted solutions may offer workflow and collaboration benefits, qualitative and quantitative returns of investment, and reduction of security-based threat surfaces applicable to content.

While disruption and digital transformation is an aim of all organizations especially where artificial intelligence and machine learning start to find tailwind, much of an organization's IT-led digital transformation will be content and unstructured data focused. While there may be a noble aim of killing off email entirely, until that day comes, entrepreneurs and forward thinking solution providers such as Canon Information and Imaging Solutions will be focused on creating synergies across a wide array of cloud-based technologies through organic Canon provided solution development and via partner-based technology alliances. In the email paradigm, perhaps the first step along the journey of digital transformation applies to an organization's need to develop a strategic cloud content management (CCM) strategy. Including email and email-based content in the center of that CCM strategy may just pay off for the enterprises of tomorrow and is certainly applicable to the Future of Work in the 21st Century.



**CANON INFORMATION & IMAGING SOLUTIONS**

### **About Canon Information & Imaging Solutions, Inc.**

Canon Information and Imaging Solutions, Inc. (CIIS), a wholly owned subsidiary of Canon U.S.A., Inc., brings together Canon's world-class imaging technologies and information management expertise to assist organizations in achieving their digital transformation objectives. With a focus on innovation, CIIS's software development and solutions delivery capabilities scale across several practice areas: Business Process Automation - including Procure-to-Pay & Order-to-Cash automation, Document Solutions, Information Management Services with a focus on content capture, management and collaboration, and Security and Infrastructure Management. With expertise in emerging technologies such as artificial intelligence, machine learning, and big data analytics, CIIS deploys its solutions in partnership with leading technology providers and offers comprehensive consulting and professional services that are trusted by organizations of all sizes.

**For more information, please contact us at [info@ciis.canon.com](mailto:info@ciis.canon.com) or visit [www.ciis.canon.com](http://www.ciis.canon.com).**

---

Canon is a registered trademark of Canon Inc. in the United States and may also be a registered trademark or trademark in other countries. //LOOKFORWARD and the LOOKFORWARD design marks are trademarks of Canon Information and Imaging Solutions, Inc. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged.

©2019 Canon Information and Imaging Solutions, Inc. All rights reserved.  
001-02-2019

**// LOOK FORWARD**