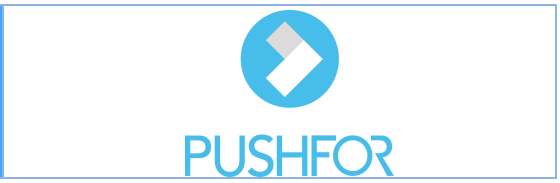
Content sharing
Whitepaper series



Making Content Intelligent

From Pushfor – a simple and safe content-sharing platform

June 2015

When we embarked on our research project to create the first Pushfor report, we wanted to find out how business professionals were managing and distributing digital content within and outside of their organisations.

To answer our questions we looked at the way business users were currently sharing content, what their concerns were and how things could be improved.

We surveyed 200 business users from different size companies – independents, SMEs and large corporations. Drilling down further, we looked at which sectors they worked in – B2B, B2C and business professionals that operated in both. The variety of different sectors and sizes is important to give a balanced view.

In a world where everything is instant – shopping is on-tap, news is published as it happens and communications is constant – it is crucial that businesses operate a seamless approach. Consumerisation trends, mobile integration and cloud delivery have transformed the way that businesses share content.

Our research intends to provide an accurate snapshot of what businesses' concerns are around sharing content and the opportunities for change and growth that exist.

John Safa
Co-founder, Pushfor

Contents

<Introduction> **1**

1. Content Sharing **3**
The need for simplicity 4
Vast amounts of content 4
Case study – Atos CEO bans email 5

2. Concerns around sharing content **6**
Case study – Dropbox puts customer data at risk 7

3. Intelligent content **8**
Analysing content 8
Analysing content continued 9
Case study – A case of stolen identity 10
Case study – A case of stolen identity continued 11

4. Conclusion **12**

5. About Pushfor **13**

Content Sharing

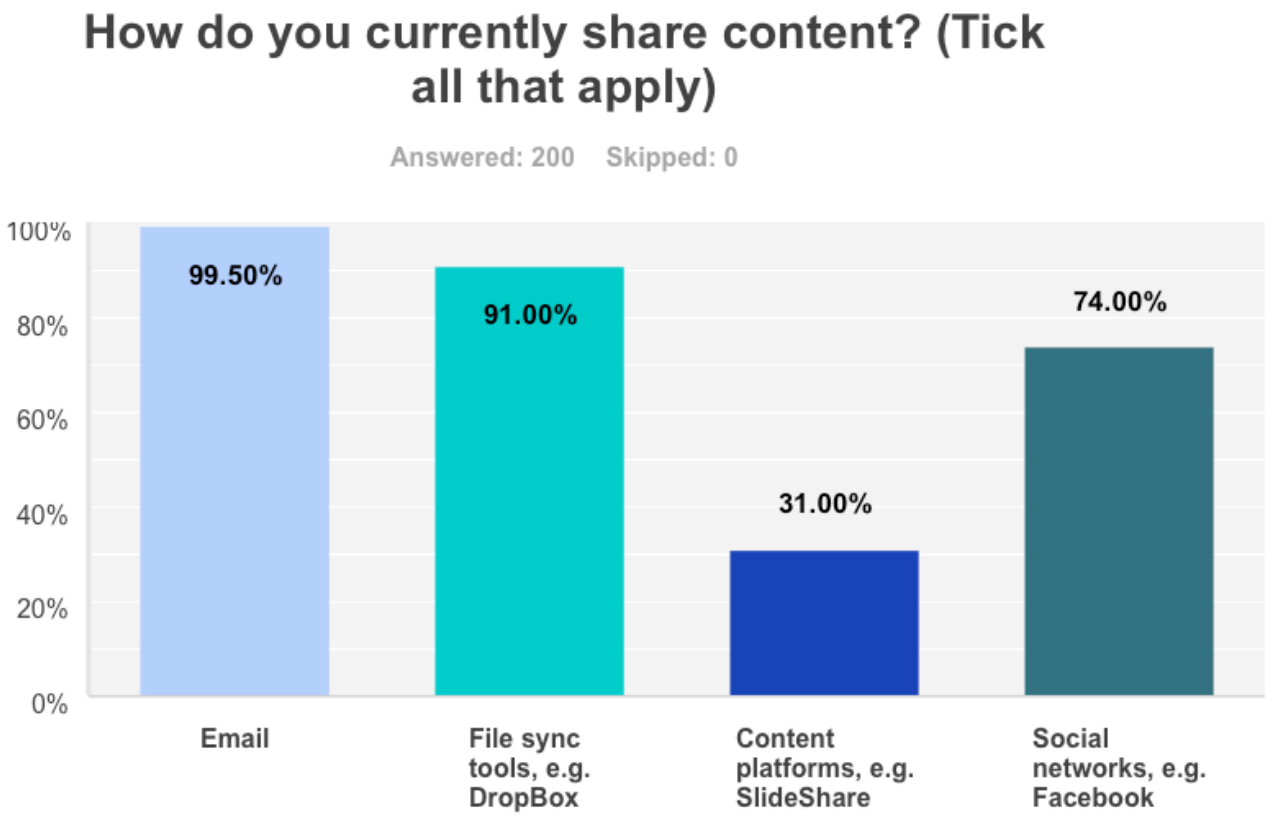
Content sharing has become ubiquitous among businesses and consumers alike; it is estimated that 27 million pieces of content are shared online each day.

There are an abundance of content sharing services available today, often used simultaneously across multiple devices, which can make content sharing complex and time-consuming.

How is content being shared?

In light of this, we asked business professionals how they share content.

The majority of respondents use email but file sync tools, such as Dropbox, followed closely behind, (91% of business professionals using these types of tools). Social media sites were the third most popular with 74%, and content platforms came last with just under a third (31%). This confirms that email is unable to provide a full service solution to today's business environment and content sharing tools are supplementing emails.



The need for simplicity

68% of respondents cited ‘ease of use’ as their biggest concern when sharing content and asked which feature they would find most useful, 74% selected ‘sending large files with ease’. These figures indicate a profound need for simplicity.

Bring Your Own Device (BYOD), is a term that was coined to describe personal smartphone usage in business. Smartphones have become integral to the workplace and business must now match a new age of professional who is connected, tech-savvy and combines their personal and work lives simultaneously. Operating cross-platform capability is vital for a simple and seamless approach.

Vast amounts of content

Every piece of content has a purpose and for content to be effective it needs to do the job it was intended to do. This ensures it is reaching its potential audience but on a much higher level it makes the content meaningful.

With the deluge of information being shared across multiple platforms, business professionals can be easily distracted. Time is one of the most valuable assets a business has, and time management can be the difference in whether a business succeeds or fails.

It is now common knowledge that email is one of the most time-consuming tools used by businesses today. Ryan Holmes, CEO of HootSuite, has dubbed it the ‘unproductivity tool’. In addition, email was not created with safety in mind and it is quickly proving to be archaic and out of touch with today’s business needs.

The reason for this is its lack of relevance. According to Atos, employees spend 40% of their time reading internal emails, which add no value to the business. Sharing content efficiently means delivering and receiving information that is meaningful.

Case study – Atos CEO bans email

In 2011 Thierry Breton, the chief executive of Atos, shocked industry professionals and the media when he announced that he was planning to put a ban on employees sending or receiving emails. He instead wanted his staff to use enterprise social apps for communicating with one another.

IT services giant Atos employs nearly 80,000 staff and the company's chief executive had estimated that barely 10% of the emails his employees received daily were useful. He also added that almost 20% were spam.

Breton felt that much of the content sent and received in his workforce was prohibiting time, "We are producing data on a massive scale that is fast polluting our working environments and also encroaching into our personal lives," he said.

"At Atos we are taking action now to reverse this trend."

Critics shunned the idea

The general consensus was that stopping email was not realistic and many felt it would have a negative impact on the company.

Despite this, Atos said the aim of the email ban was for the company to "transform towards a social, collaborative enterprise where we share knowledge and find experts easily in order to respond to clients' needs quickly and efficiently, delivering tangible business results."

Did it work?

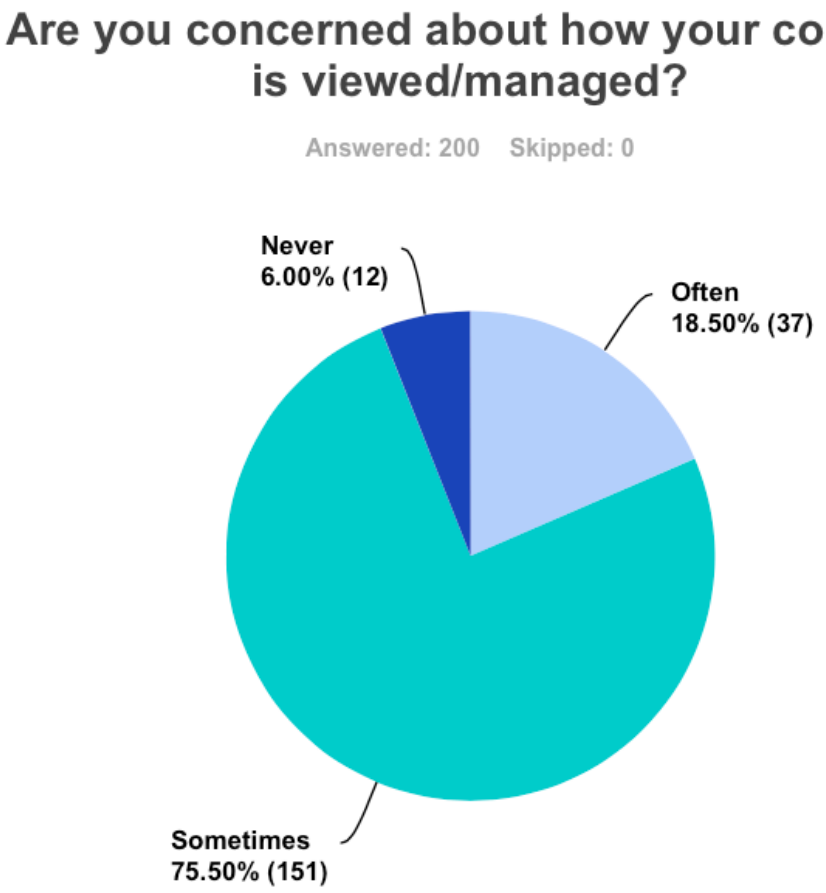
Fast forward four years and where is Atos today with the email ban initiative, and how has it affected the company so far?

Atos has not yet rolled out the no-email approach across the entire company but it has reduced it by 60%, here is what happened as a result:

- Free cash flow increased year on year from €267 million to €365 million, earnings per share increased more than 50 percent
- Selling, general, and administrative costs declined from 13% to 10%
- Email dropped from 100 per mailbox per week to fewer than 40 – a 60% decrease

Concerns around sharing content

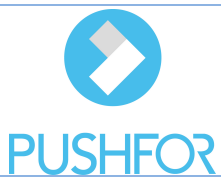
Not only has the amount of content we share increased but concerns are now high surrounding privacy and the way content is shared. Our research shows that almost all respondents share confidential or sensitive information and 94% are concerned about how their content is viewed.



These figures demonstrate the importance of safety when sharing content, and it is not difficult to see why. High profile leaked-document cases in both businesses and consumers continue to flock the news and smaller businesses are also vulnerable to online attacks.

A separate study from Zurich found that 45% of SMEs are concerned about tech vulnerablilities – including cyber security, data integrity and mobile devices.

Our research found that 59% of business users felt file sync services were the safest way to share content. Email came second with 35.5%, followed by social media and content platforms, which gathered 4% and 1.5% respectively.



Case study – Dropbox puts customer data at risk

Although the majority of those surveyed felt that file sync services, such as Dropbox, were the safest way to share content, it's not entirely the case.

Last year Dropbox received backlash after it was revealed that the provider of file syncing services was putting customers' sensitive data at risk. It was found that links created by Dropbox users were easily accessible and allowed documents, only intended for trusted sources, to be viewed by third parties.

Dropbox's competitor Intralinks had been carrying out a routine Google Adwords campaign when it stumbled upon the major flaw. Intralinks was able to access confidential files including bank records, mortgage applications and business plans.

How links could be accessed

If a document contained a link to a website, the referral data for that website would store a link to the document, which could be clicked on and viewed. Secondly, if a link was put into a search engine and not a URL bar, Google Adwords would see this as a search term, again allowing the document to be accessed.

It was also revealed that Intralinks had informed Dropbox of the problem in confidence in November 2013 but after the company made no attempt to resolve the issue, Intralinks took it public in May 2014.

In response to this, Dropbox said that it had resolved the issue for any new links, but that existing links had been disabled.

Dropbox commented: "For all shared links created going forward, we've patched the vulnerability. For previously shared links to such documents, we've disabled access entirely until further notice,"

"We realise that many of your workflows depend on shared links, and we apologise for the inconvenience. We'll continue working hard to make sure your stuff is safe and keep you updated on any new developments."

Where the problem lies

The main problem with this is that Dropbox doesn't provide password protection or expiry dates for links, which would increase document security considerably. According to research from PwC and the UK Department for Business, cyber attacks cost businesses as much as £1.15m per incident.

Intelligent content

The way we share content needs to keep pace with businesses' ever-changing requirements; it should be mature and sophisticated.

As shown throughout our whitepaper, the following aspects are important when sharing content:

- Ease of use
- Safety
- Relevance
- Productivity

Those are some of the crucial points that help transform average content into intelligent content. But what matters just as much are privacy and analytics tools.

When SnapChat launched, it offered the world a new concept – a way to send content with a short shelf life, offering an abundance of privacy and safety. When the same concept is applied to business, the benefits are clear.

As our research suggests, most businesses share confidential content. When that information is shared digitally, they no longer control the data and, instead, recipients are able to do with it as they please. On the contrary, when content has an expiry date it is safe; it cannot fall into the wrong hands or be duplicated.

Analysing content

Analytics help to shape a business; they represent customer data, financial information and are the catalyst for business growth. For this reason, analytics can be a powerful tool when sharing content.

Businesses that use analytics when sharing information are given unique insight into how well they're performing. They can use this data to discover new opportunities, and make substantial cost savings.

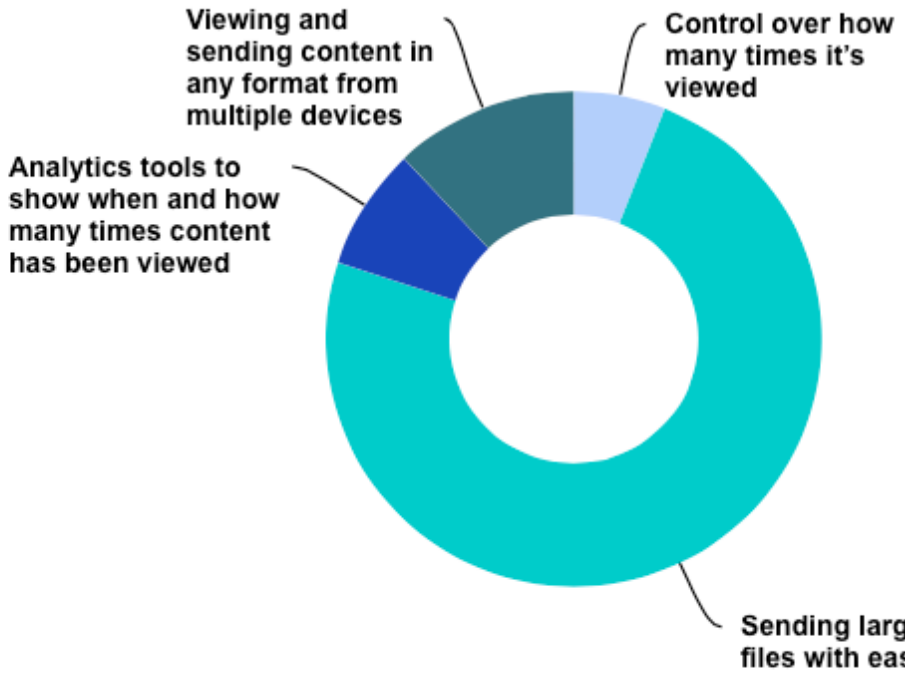
According to our survey, 8% of respondents cited analytics as the most useful tool when sharing content. This will probably increase by next year as businesses become more aware of the value analytics tools can add when sharing content.

6% of businesses would find it most useful to be able to control how many times content is viewed. While this figure is low, it is not a surprise. The current landscape is changing with both businesses and consumers embracing the idea of having more control over how their content is seen.

It is likely that these tools will be integrated into businesses over the next couple of years, and when our follow-up whitepaper is released next year, we are expecting to see these figures rise significantly.

Which feature would you find most useful when sharing content?

Answered: 200 Skipped: 0



Answer Choices	Responses	
Control over how many times it's viewed	6.00%	12
Sending large files with ease	74.00%	148
Analytics tools to show when and how many times content has been viewed	8.00%	16
Viewing and sending content in any format from multiple devices	12.00%	24

Case study – A case of stolen identity

While businesses are slow to grasp the importance of adopting control tools to protect content, it seems consumers are learning the hard way.

A married 25-year old from Brighton was recently horrified to find out that an imposter had cloned her identity and was using her images to lure men into online relationships.

Ruth Palmer discovered that she had become a victim of online identity fraud after a friend spotted the scammer's social media profile, which contained an image of Mrs Palmer.

It was revealed that the mystery person had stolen almost 1,000 pictures of Ruth Palmer, and was using them on Instagram and Twitter to dupe unsuspecting men into relationships.

Known only as 'Leah Palmer', the perpetrator went as far as setting up fake social media accounts of Mrs Palmer's mother and a friend, in an attempt to make the profiles appear realistic.

Increasingly common

While Ruth Palmer's case of online identity fraud is bizarre, it's not uncommon and is quickly becoming a reality for many other people.

MTV's reality TV show Catfish, which was launched in 2012, helps people determine whether or not their lovers who they've met online are being honest about their identity. This often involves shocking revelations, with victims being enticed into relationships with the same tactics used by Ruth Palmer's impostor.

Now into its fourth season, MTV's Catfish has become a global hit, and a UK version of the show is set to launch this year.

Risky environments

Ruth Palmer's case of stolen identity is a sharp realisation of the risks associated with sharing personal content online.

Even with the strictest privacy settings in place, social media sites like Facebook, Twitter and Instagram do not offer a high level of security and content can be easily stolen.

Ruth Palmer's shift to safe online sharing

Ruth Palmer has been faced with all kinds of problems as a result of using social media. She is now looking for a safer, more private way to share her life with family and friends and, as a result, has started to use the Pushfor app.

Here are her comments on using Pushfor:

"It is great to see a platform where the primary focus is the safety of content. Our online world has been crying out for this type of data sharing for some time."

Mrs Palmer went on to say, **"Pushfor will revolutionise the way in which we share our data with colleagues or friends. It's an app that is trustworthy and honest in regards to the privacy of personal and professional details and documents."**

Pushfor gives Ruth Palmer safety and control over how her content is shared. It offers privacy permission rules; allowing her to send self-expiring content and set limitations on how many times it can be viewed.

In addition, Pushfor lets users recall messages, or 'pull' them as the company describes. Content, such as videos, photos and documents, can be pulled after it has been sent – removing it from the recipient's device.

Conclusion

It is clear from our research that the way business users share content needs improving. Safety, simplicity and productivity are top on businesses' priority lists and the current methods of sharing content are not meeting the demands of the content owner.

The adoption of social tools in business has seen huge transformations in the way we run our working lives, increasing the amount of content we share as a result. Consequently, the sheer volume of content being shared means it is imperative for information to serve a purpose. It is only when this happens that communication becomes collaboration.

While there are many tools available that solve certain issues, workload becomes problematic when businesses use several platforms for different uses. To meet the highest productivity rate, business professionals must adopt content sharing tools that meet their overall needs and not just a specific need.

The Pushfor app enables consumers to share content in an innovative but simple way. It allows users to connect their file storage service to Pushfor and then share any content with full privacy controls, safety and download restrictions – driving ease, productivity and protection.

To summarise, a business should be able to share content with ease and control, and, perhaps most importantly, safely – this is why Pushfor will soon become available for businesses.

John Safa, Co-founder Pushfor

About Pushfor

Pushfor is a private cloud-sharing platform that gives users full safety and control over their content. Officially launched in May 2015, Pushfor makes cloud-sharing simple by allowing users to send content of any size, any file type, from any device, with ease. The Pushfor app combines intelligent analytics tools with privacy permission rules to offer users visibility and control when sharing content.

Media contact:
Stephanie Dunleavy
PR Manager
+44 7925 446 126
Stephanie.dunleavy@straightmessage.com

Other enquiries:
Scott Smull
CEO
+44 7539 037 404
Scott@pushfor.com