Workshare

DATA GUARDIAN:

DETECTING BUSINESS RISK 2014

EMEA KEY PARTNER
Eagle Networks
By Blue Eagle Technology
Via Micanzi, 9 Brescia
Tel. +39 030 2010825
Email: sales@eaglenetworks.it
www.eaglenetworks.it/workshare

Workshare

DETECTING BUSINESS RISK

Contents

INTRODUCTION

Workshare conducted a survey to determine how everyday file sharing practices are exposing sensitive corporate data to risk. Over 800 respondents answered questions on the commercial value of a document, their sharing habits in light of this, and the security threats this poses. Those surveyed represented a global cross section of knowledge workers for whom the documents resulting from creation, collaboration, and sharing constitute a large proportion of their intellectual property (IP) and corporate assets. Highly regulated industries such as the financial and legal sectors were particularly well represented. Respondents answered questions on the following topics;

IDENTIFYING AND SHARING HIGH-VALUE DOCUMENTS

- Which device(s) do you use for work?
- Does your employer have a 'Bring Your Own Device' policy or allow you to use personal devices for work?
- Do you consider some documents to have more commercial value than others?
- Do you consider the content of a document when it comes to sharing it?
- What adds more value to a document?

SECURING HIGH-VALUE DOCUMENTS

- How do you treat documents you consider to be of high value when sharing them?
- How often do you receive emails with attachments that were not intended for you?
- Do you remove hidden sensitive data (metadata) from documents before sharing?
- Can you set limits on how long the recipient has access to that document/file?
- Have you ever forwarded an email with an attachment (document/file) without reading the attachment first?
- Do you clean the document of hidden sensitive data (metadata) before forwarding it on?
- Have you ever logged onto an unknown Wi-Fi/internet connection to share a document/file quickly?

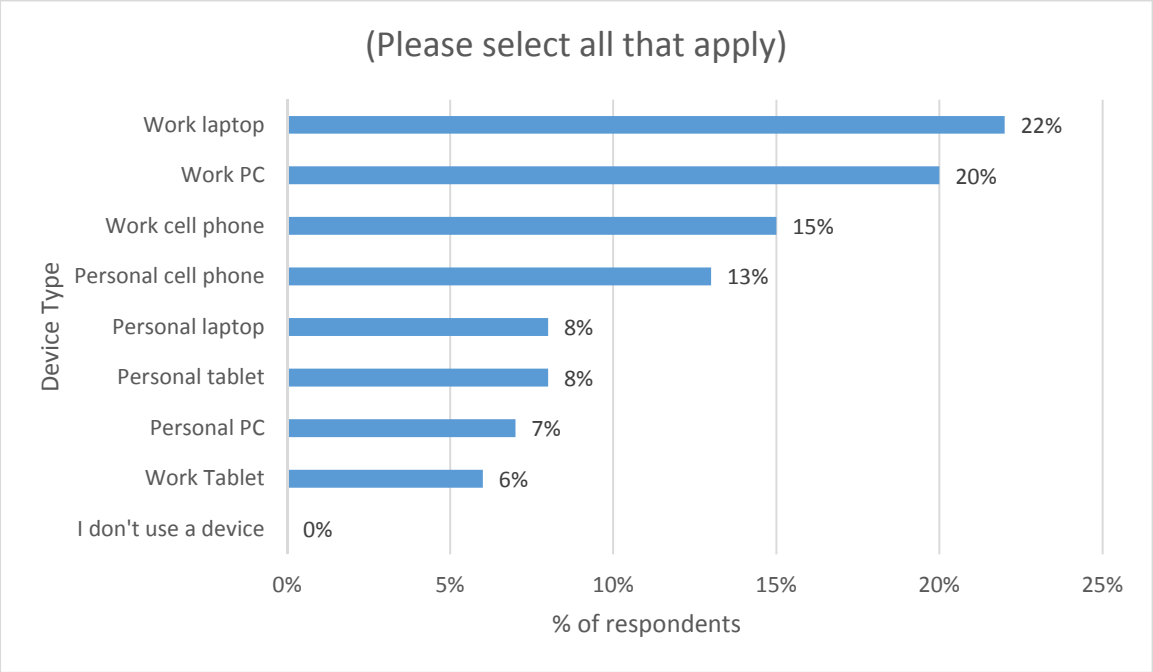
WHO IS RESPONSIBLE FOR COMPANY DATA

- In your opinion, who is most responsible for ensuring that sensitive company content isn't inadvertently leaked?
- Does your company have a 'Bring Your Own App' (BYOA) policy or allow you to use the mobile apps you want for work?
- Do you still use the apps you want/need for work?
- Is your company aware of the mobile apps you use?

1.0 IDENTIFYING AND SHARING HIGH VALUE DOCUMENTS

Respondents were asked questions about what devices they use for work to share sensitive content, whether they believe different content has higher or lower commercial 'value,' and whether they consider this 'value' when sharing internally and externally.

1. Fig. 1.1: Which device(s) do you use for work?

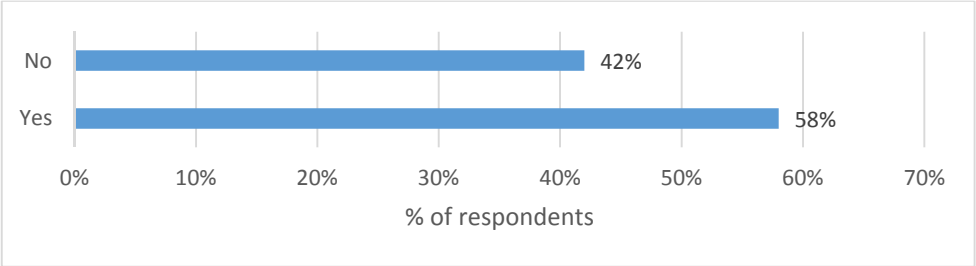


- The majority of respondents use at least one device provided by their organization in the workplace (63%). Generally, work PCs and devices that have been sanctioned by IT groups represent the lowest risk to corporate content due to a variety of security methods, including VPNs, encryption, backup, firewalls, user and policy management, and centralized data control.

- However, 36% of respondents use some form of personal device for work activities, which can mean that IT groups lose control of corporate data on unsanctioned and unprotected devices. This means that for 36% of respondents, IT groups have no control over corporate data and risk exposing it to data leakage or loss.

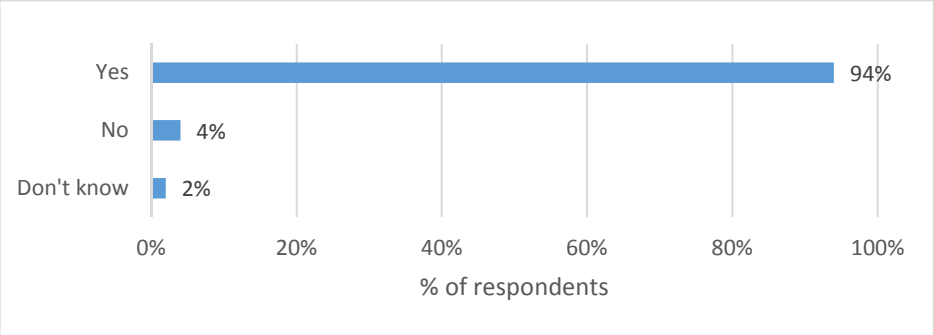
- There are Bring Your Own Device (BYOD) initiatives in place in many organizations in an attempt to enforce a level of control over corporate content being shared from personal devices. These include the adoption of secure file sharing and sync applications built for the enterprise that enable remote collaboration while securing content.

2. Fig. 1.2: Does your employer have a 'Bring Your Own Device' policy or allow you to use personal devices for work?



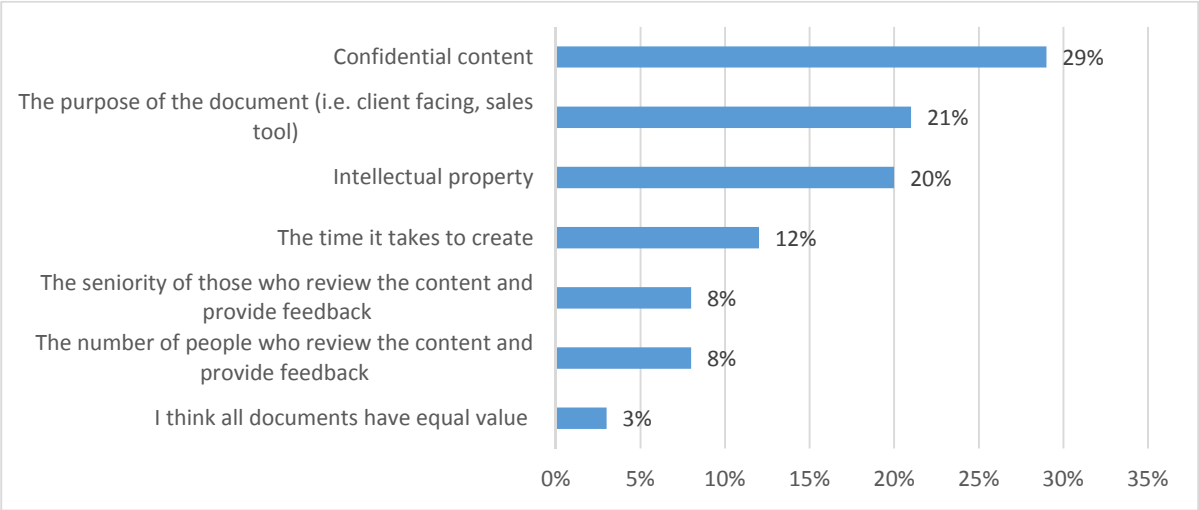
- 42% of respondents answered that their employer does not have a BYOD policy or allow them to use their personal devices for work. This means that almost half of the organizations represented are not providing policies or sanctioned applications that ensure control and security of corporate content.

3. Fig 1.3. Do you consider some documents to have more value than others?



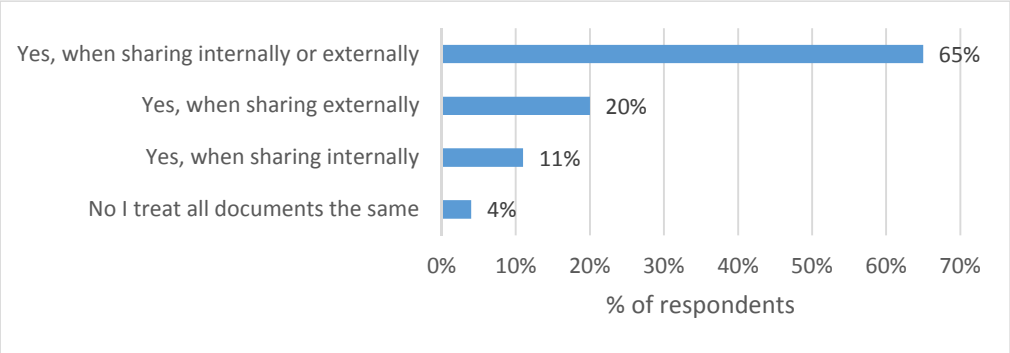
- When asked if they consider some documents to have more commercial value than others, an overwhelming 94% of those surveyed answered 'yes'. This suggests that they believe there can be 'low-value' and 'high-value' documents, with factors that contribute to a document being considered more or less valuable.

4. Fig. 1.4: If you answered yes, what adds more value to a document?



- Out of the 94% who consider some documents to have more value than others, the majority of respondents (29%) believe that it is confidential content that adds most value.
- This is closely followed by 21% citing that it is the purpose of the document and 20% asserting that it is the intellectual property a document contains that increases its value.

5. Fig. 1.5: Do you consider the content of a document when it comes to sharing it?

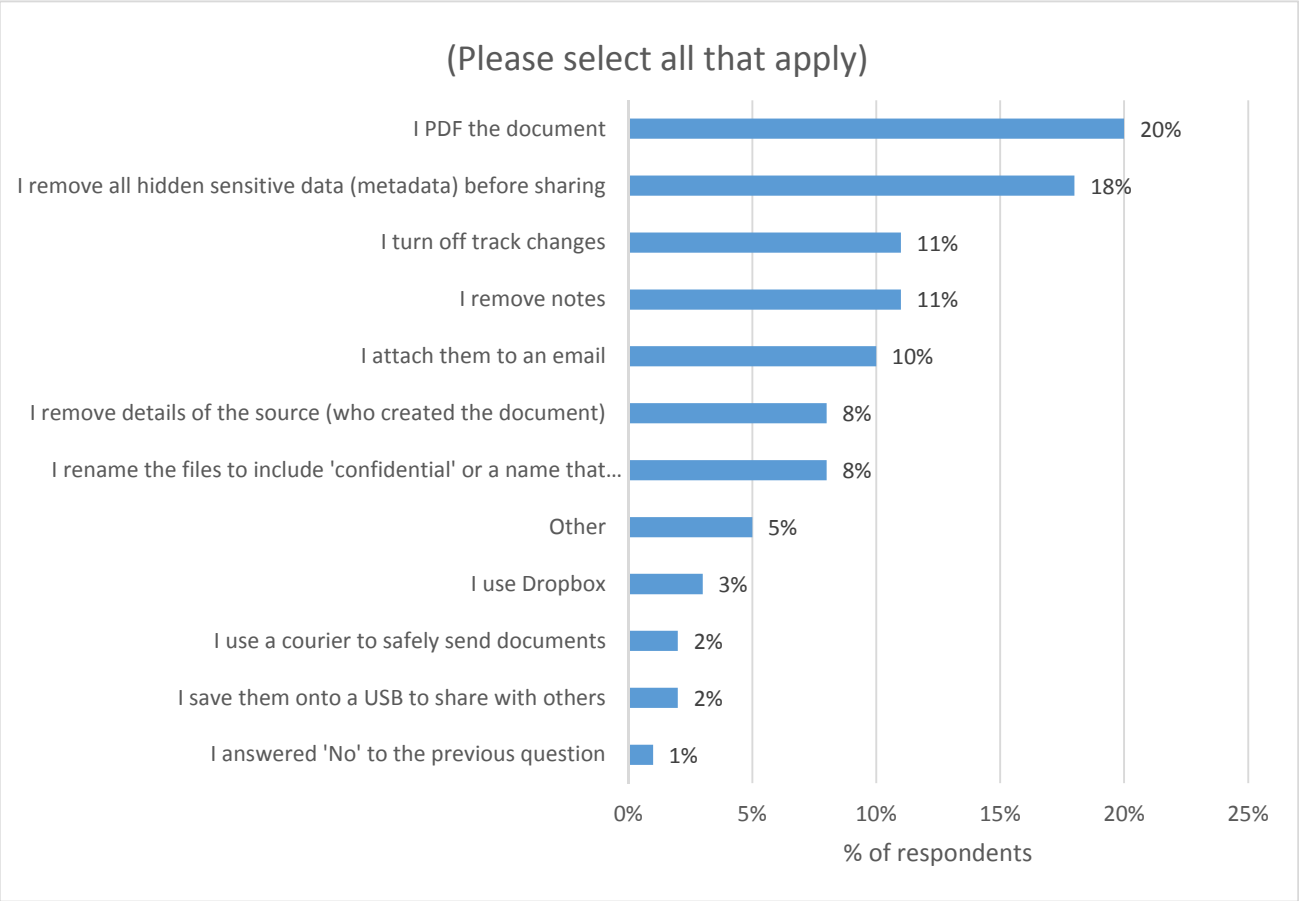


- 35% of respondents don't consider the content of a document when sharing it both internally or externally.
- Those that only consider the content of a document when sharing it externally (20%) appear to be unaware of the security risks inherent with sharing a file internally. Data loss is still a clear and present risk through other employees sharing or forwarding their documents unsecurely.
- 11% of people are cautious when sharing documents internally, suggesting that they are more concerned with how colleagues consume and interpret their content, rather than its security, which is usually key a consideration for businesses when sharing sensitive or high-value content externally.
- The results raise questions around the security of corporate content being shared internally and externally by employees, as can be seen in Figure 2.1 below.

2.0 SECURING HIGH-VALUE DOCUMENTS

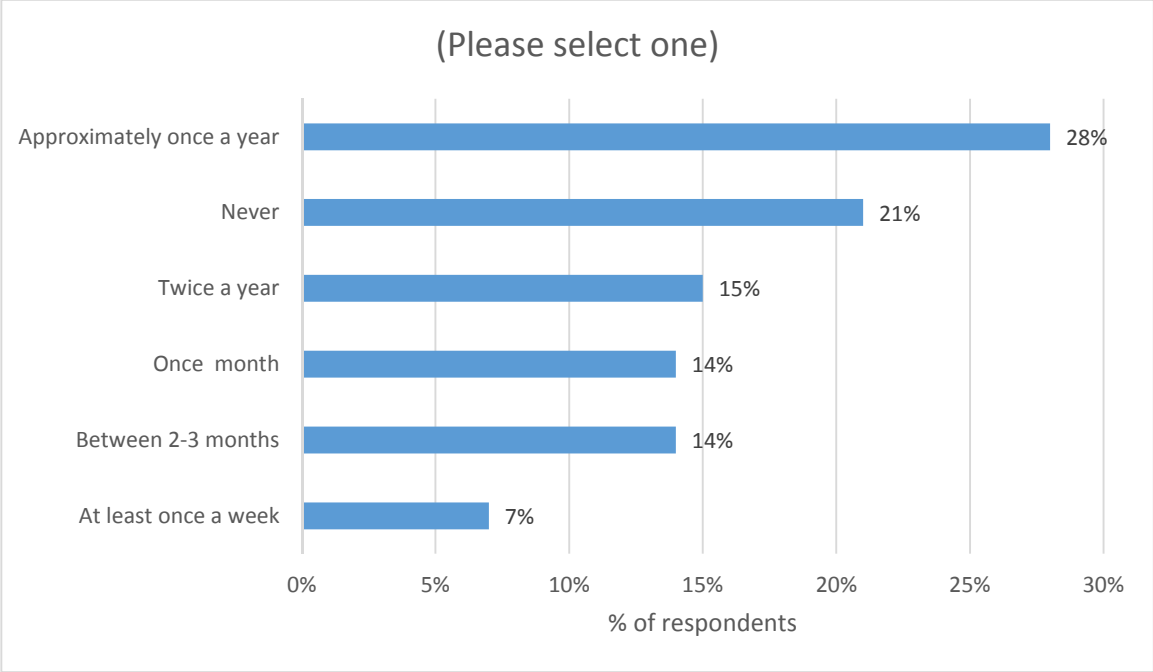
In light of the commercial 'value' the respondents do or do not place on documents, questions were asked regarding how they handle these documents when it comes to sharing and accessing them, both inside and outside of the corporate network.

1. Fig. 2.1: If you answered yes to the previous question, how do you treat documents you consider to be of high value when sharing them?



- 80% of respondents put high-value corporate files at risk due to unsecure file sharing methods. This means that over 80% of documents sent contain hidden or sensitive data (metadata), which could include details about who originally created the document, track changes, and review comments in a Word document, or even financial information hidden in an Excel spreadsheet. If exposed, these details could cause irrevocable damage to a company's reputation and competitive advantage and result in costly data breach fines.

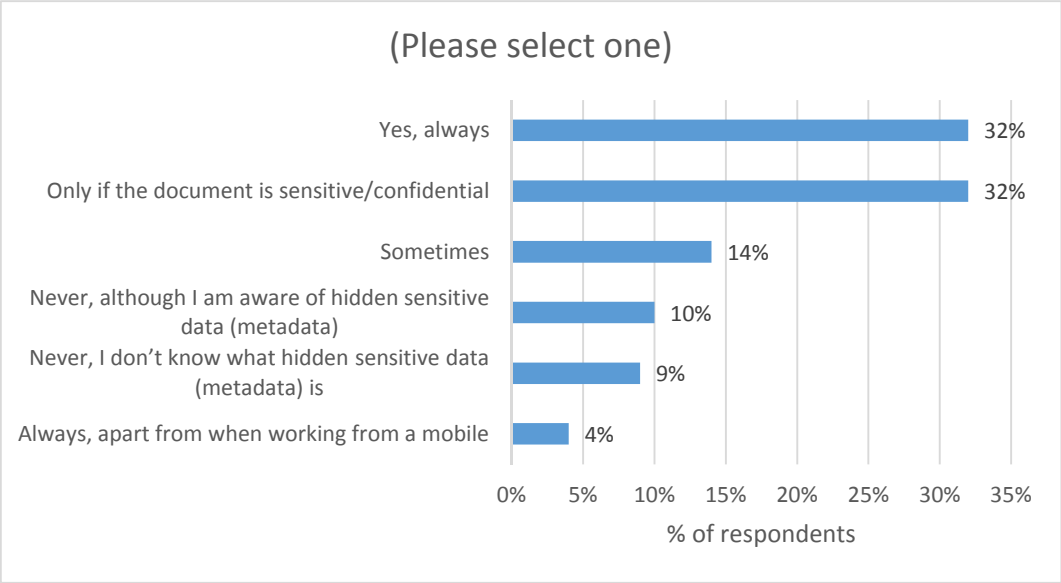
2. Fig. 2.2: How often do you receive emails with attachments that were not intended for you?



- The same risk of data loss is evident from the amount of respondents who receive email attachments that are not intended for them, with 80% of respondents stating that they do. With no way to effectively recall those documents, the content within them is lost with no way of tracking what happens to it after hitting send.

- The results suggest that there is a significant amount of valuable and sensitive corporate content in the wrong hands that could continue to be shared or used maliciously. If leaked, this data could cause significant damage to client relationships and business, as well as breach compliance mandates.

3. Fig. 2.3. Do you remove hidden sensitive data (metadata) from documents before sharing?

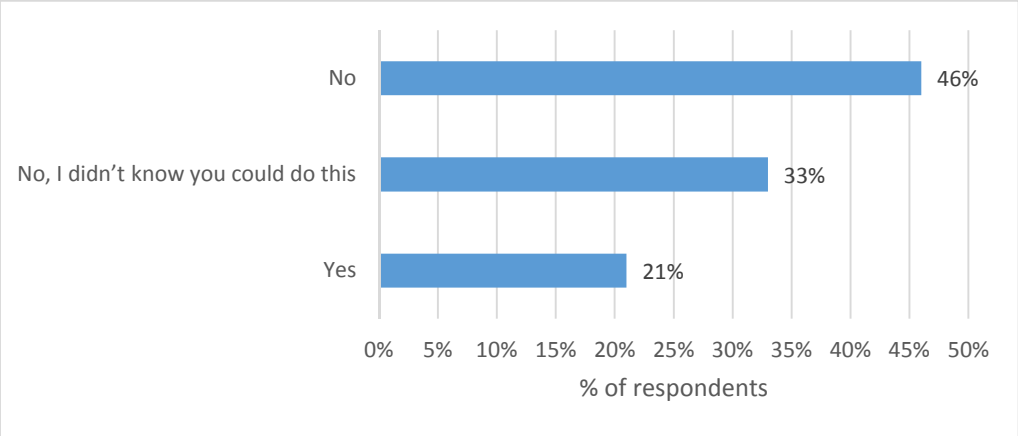


- Almost 70% of respondents do not ensure that metadata is removed from a document before sending, with only 32% removing it only if they deem the content itself to be sensitive or confidential

- Only 4% stated that they usually remove metadata but don't or do not have the capability to do so when sharing from a mobile device.

- 10% are aware of what hidden sensitive data (metadata) is but still don't remove it, suggesting that more education and controls need to be put in place to ensure that sensitive data is not being compromised. This finding also raises concerns over employees taking security into their own hands and deciding what content needs to be cleaned of sensitive data and when.

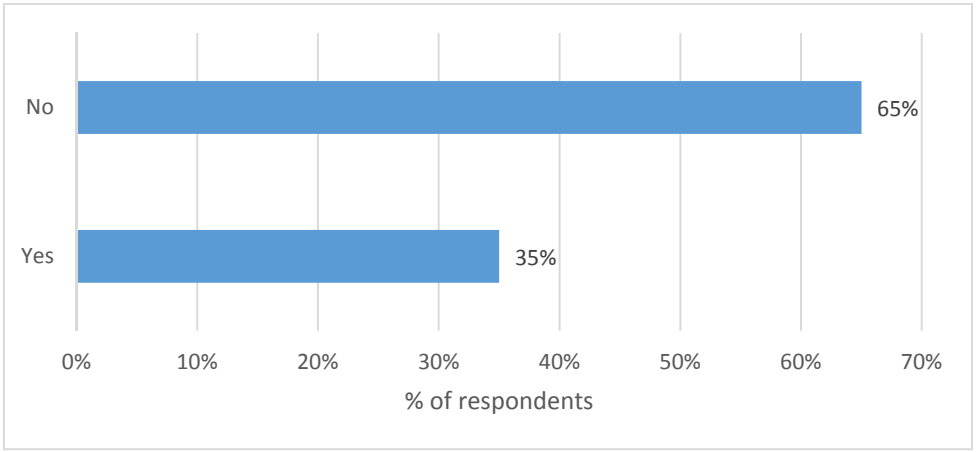
4. Fig. 2.4 Can you set limits on how long the recipient has access to that document/file?



- 79% of information professionals cannot control how long their recipients have access to the content they send to them. This means that once shared, recipients can keep the shared content for an undefined period of time, with the owner having no way of restricting or rescinding access and no visibility over how that content is then used or shared.

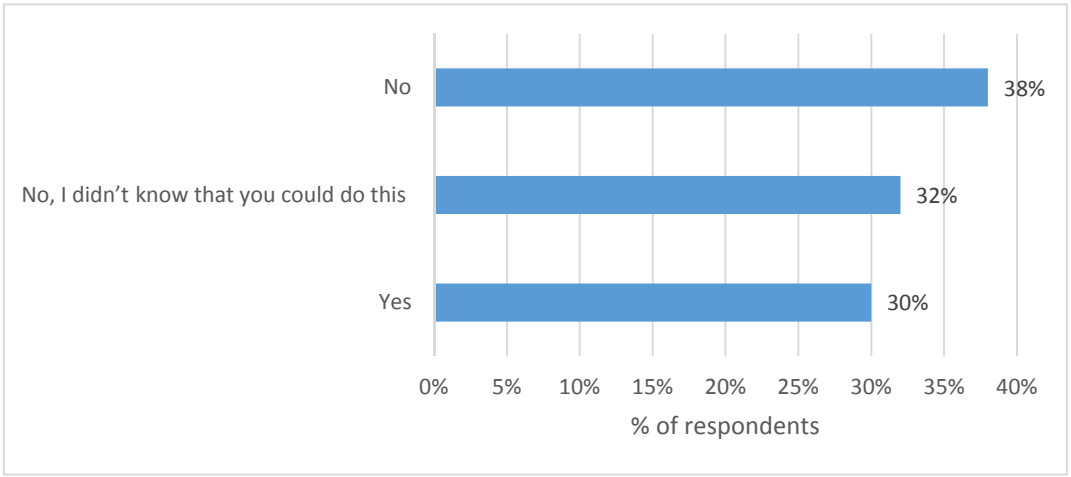
- For competitive businesses, losing or exposing confidential corporate content such as intellectual property puts business at considerable risk, especially if this information falls into competitors' hands.

5. Fig. 2.5: Have you ever forwarded an email with an attachment (document/file) without reading the attachment first?



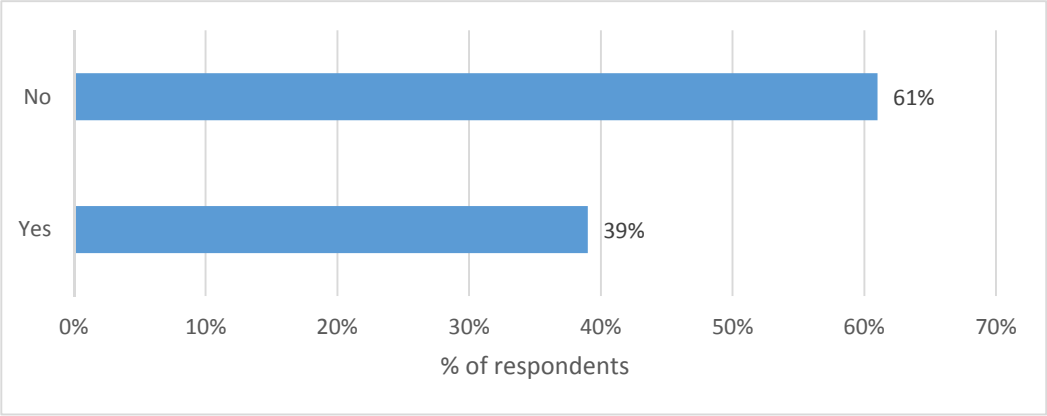
- 35% of respondents have forwarded an email with an attachment that they didn't read or check before sending. This finding suggests that people are unknowingly sharing content that may contain undetected hidden data (metadata), putting corporate information at risk.

6. Fig. 2.6: If you answered yes to the above, do you clean the document of hidden sensitive data (metadata) before forwarding it on?



- As highlighted in Figure 2.6 out of the 35% in Figure 2.5 that forward emails with attachments without reading the document first, a staggering 70% do not clean it of metadata. This finding proves that documents forwarded are highly likely to contain hidden sensitive data, posing significant security risks to the organization.

7. Fig. 2.7: Have you ever logged onto an unknown Wi-Fi/internet connection to share a document/file quickly?



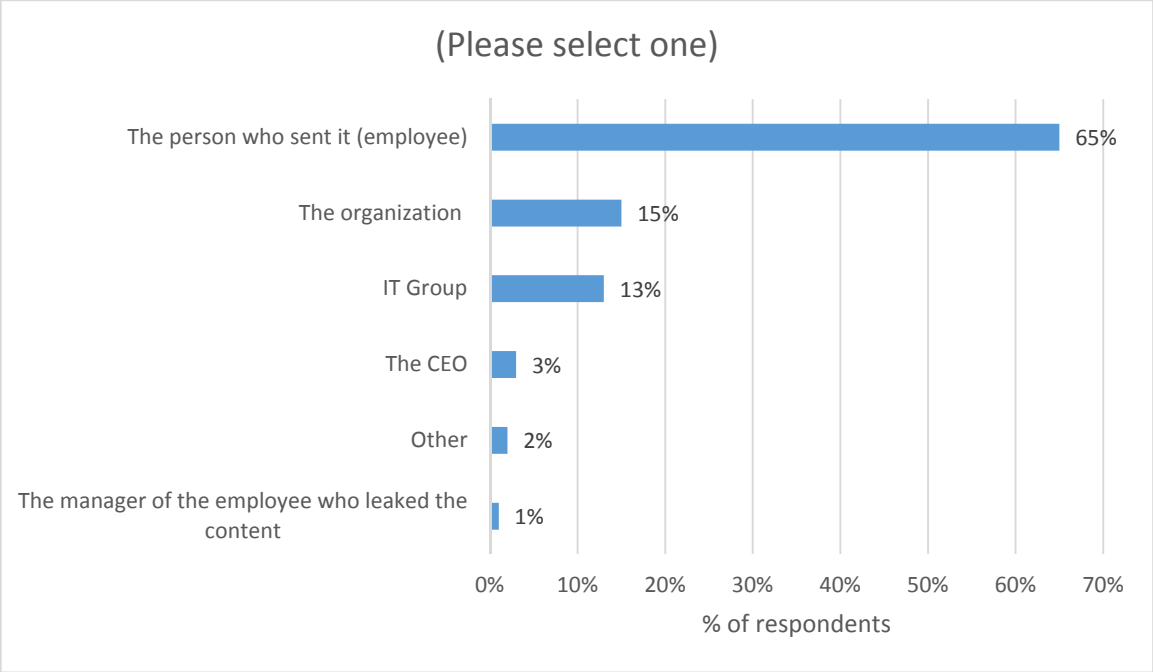
- Almost 40% of respondents use unknown Wi-Fi and internet connections to share a file quickly.

- Unlike the secure, controlled networks used at work, unknown Wi-Fi networks are highly risky as they not only pose a threat to the security of devices through malware, but also increase the chance of snooping and intercepting what is being shared. Indeed, many networks purporting to be “free Wi-Fi” often fraudulently ask users to log in so that they can capture personal information and undertake malicious data theft, making this finding extremely concerning for businesses and IT groups.

3.0 WHO IS RESPONSIBLE FOR COMPANY DATA

When it comes to securing corporate content, whose responsibility is it? The knowledge workers were asked whom they deemed responsible for securing sensitive corporate data, as well as if they had sufficient support from IT in ensuring they could do so through Bring Your Own Application (BYOA) initiatives.

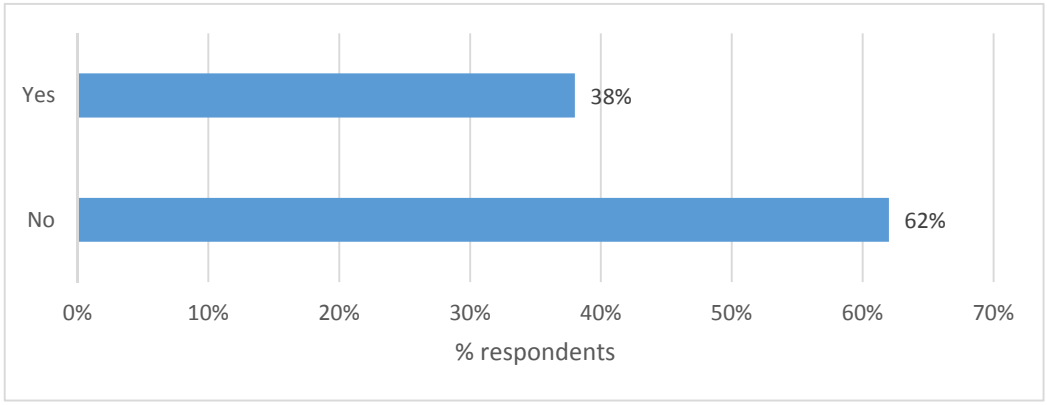
1. Fig 3.1: In your opinion, who is most responsible for ensuring that sensitive company content isn't inadvertently leaked?



- 65% of respondents see it as the responsibility of the sender to ensure that sensitive company data isn't inadvertently leaked. But as has been proven in this report so far, many employees are not practicing safe sharing practices. This raises concerns about whether those who they have identified as being responsible for removing hidden data (the senders) are effectively doing so.

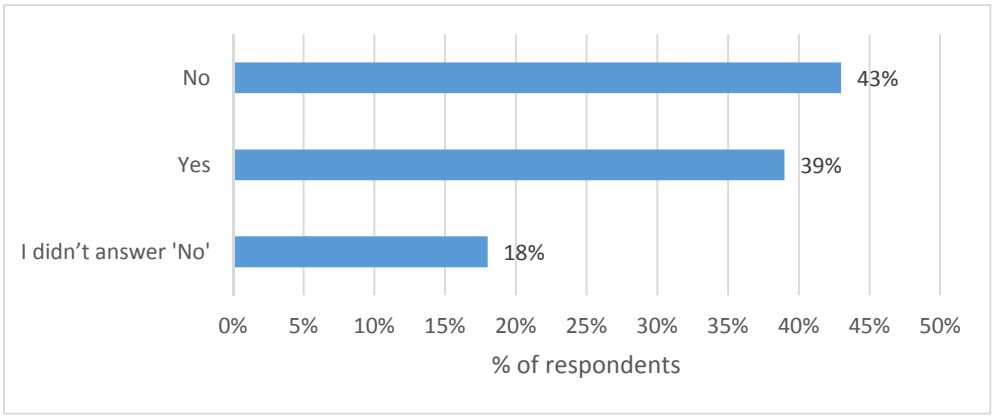
- A third (35%) of respondents did not see securing company data as their responsibility, and as such it can be assumed that they will undertake riskier sharing behaviors as they believe it is down to someone else within the organization to ensure it is secure.

2. Fig. 3.2 Does your company have a 'Bring Your Own App' (BYOA) policy or allow you to use the mobile apps you want for work?



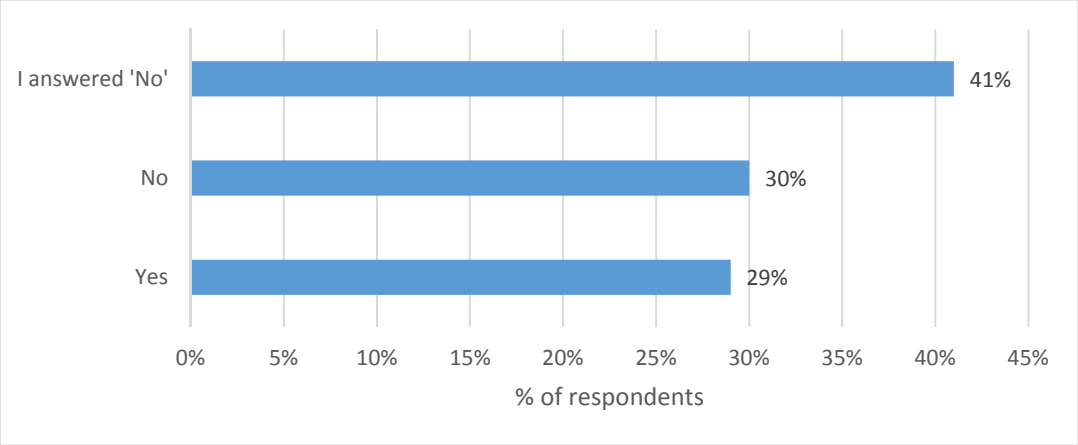
- Only 38% of those surveyed have a BYOA program, where applications are sanctioned for use by IT groups, or are allowed to use the mobile apps they want to for work.
- This indicates that 62% of those surveyed don't have a BYOA policy in place or are banned from using the applications they want to for work.

3. Fig. 3.3: If you answered no, do you still use the apps you want/need for work?



- However, out of the 62% of survey respondents who don't have a BYOA policy or are not allowed to use the applications they want, 39% still do use the applications they want to.
- This means that IT have no knowledge or insight into what applications these employees are using to share sensitive corporate documents and as such have no control over it, and cannot ensure policy is enforced, as can be seen in Fig 16.

4. Fig. 3.4: If you answered yes, is your company aware of the mobile apps you use?



- 62% of organizations don't let users use their own apps for work, but despite this 39% of users still do, with 30% of those respondents doing so without ITs knowledge. This highlights a need for IT to provision easy-to-use enterprise alternatives to the consumer applications that users are comfortable with, in order to regain control of company data.

SUMMARY AND CONCLUSION

This report exposes the stark reality of risk for businesses associated with employees sharing high-value business documents. Even though 94% of knowledge workers recognize that some documents have more commercial value than others, only 1 in 5 indicate that they use secure methods to share them. In addition, 68% of professionals are exposing their businesses' most confidential information to extreme risk by failing to remove hidden data (metadata) from shared documents.

But whose responsibility is it to ensure corporate data is kept secure at all times? 65% of respondents believe it's their responsibility to ensure that sensitive company information is not leaked, but 80% of them are using unsecure file sharing methods, putting corporate data at risk.

More and more employees are beginning to use their own devices and applications in the workplace to share corporate content. As seen in the report, if not sanctioned by IT, this sharing behavior leads to increasing levels of commercial and compliance risk as data leaves the confines of the corporate network without the control of IT groups. There is a definite need for IT to regain control over company data and educate users about the risks inherent in sharing high-value content, while enabling them to work the way they want.

This can be achieved by providing users with applications to detect risk and applications that enable them to remove hidden sensitive data prior to sharing, as well as protecting their corporate data when working from personal mobile devices.

To find out more about how to protect sensitive documents, visit
for English: http://www.workshare.com/products/protect
for Italian: https://www.eaglenetworks.it/workshare

ABOUT WORKSHARE

Workshare is a leading provider of secure enterprise file sharing and collaboration applications. Workshare allows individuals to easily create, share, and manage high-value content in cloud storage anywhere, on any device. Workshare enhances the efficiency of the collaborative process by enabling content owners to accurately track and compare changes to shared documents from contributors simultaneously. Workshare also reduces the commercial risk posed by inadvertently sharing confidential or sensitive documents. More than 2 million professionals in 70 countries use Workshare's award-winning desktop, mobile, tablet, and online applications.

For more information visit http://www.workshare.com or follow Workshare on Twitter at http://www.twitter.com/workshare.
For Italian version: https://www.eaglenetworks.it/workshare