



## The High-Cost of Mobile Business Users' Rogue IT Practices

---

**David Lavenda**

Vice President, Product Strategy

## Contents

Executive Summary .....	<b>3</b>
Key Findings .....	<b>3</b>
What Is Keeping IT Professionals Up At Night? .....	<b>5</b>
Four in 10 Employees Ignore Their Company's IT Policy .....	<b>5</b>
More Than a Quarter of Business Users Admit to Causing a Security Breach .....	<b>7</b>
The High Cost of Rogue IT .....	<b>7</b>
In SharePoint organizations alone, businesses waste \$904,671,666 by duplicating file sync/sharing services via Dropbox. This money could be better spent putting 40,639 students through one year of college.....	<b>10</b>
Survey Demographics .....	<b>11</b>
About harmon.ie .....	<b>13</b>

## Executive Summary

'Rogue IT' is a phenomenon that occurs when workers circumvent organizational controls by exploiting unsanctioned IT resources that are outside the supervision of corporate IT. For example, many workers store corporate documents on publicly-available file sync and store services, such as Dropbox.

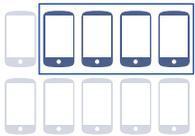
As organizations become increasingly mobile, the incidence of rogue IT behavior is most certainly intensifying...by just how much, is not clear.

So, in an effort to quantify the impact and highlight the scope of rogue IT practices, as well as gauge the damages it is causing organizations, enterprise mobile application provider [harmon.ie](http://www.harmon.ie) (pronounced 'harmony') commissioned a survey of 500 business IT users working in US and global companies. The survey was fielded August 13th -22nd, 2013 by online market research firm uSamp (United Sample). See Survey Demographics for details about the sampling population.

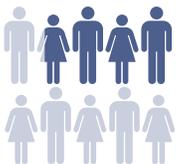
## Key Findings

What is the #1 worry of IT professionals today? The survey found that fear of a data meltdown due to compromised documents lost via unsecured file sync services tops the list, with malware downloaded via third-party apps as #2; viruses ranked third.

According to the survey results, this fear is well-founded because:



**41% of US mobile business users** have used unsanctioned services such as Dropbox or Google Docs to share or sync files, despite 87% saying they are aware that their company has a document sharing policy that prohibits this practice. When extrapolated to the general population, this translates into **14,937,553** rogue business users in the US alone.<sup>1</sup> This is akin to every man, woman and child living in the greater Los Angeles metropolitan area ignoring corporate policies to get their work done.<sup>2</sup>



**More than one third (38%) of respondents** said that a document shared using an unsanctioned service reached an **unintended recipient**, and **one in four (27%) reported a data breach** and negative consequences as a result. So odds are uncomfortably high that if employees are using unsanctioned services, they'll make a big – and potentially costly – mistake.

The cost to remedy data leakage resulting from handling company documents using unsanctioned services is estimated to total **\$1,849,628,696**<sup>3</sup>.

In SharePoint organizations alone, 40% of business users rely on Dropbox to share or sync documents while working on the go, **wasting** another **\$904,671,666 a year** by duplicating file sync and sharing services.<sup>4</sup>

<sup>1</sup> The total population of white collar workers in the US is 55,201,600.  
Source: <http://kff.org/other/state-indicator/blue-and-white-collar-workers/>.  
-66% of employees now use two or more devices every day, including desktops, laptops, smartphones and tablets, according to Forrester Research.  
- 55,201,600 x 66% x 41% = 14,937,553 people.

<sup>2</sup> Source: [http://en.wikipedia.org/wiki/List\\_of\\_metropolitan\\_areas\\_by\\_population](http://en.wikipedia.org/wiki/List_of_metropolitan_areas_by_population)

<sup>3</sup> # US workers that use mobile devices to get work done: 55,210,160 \* 0.66 = 36,438,706  
36,438,706 x 27% that have experienced a security breach when handling documents using unsanctioned services = 9,839,450 incidents.  
- According to Symantec, the cost per lost or stolen record is \$188.  
Source: [http://www.symantec.com/about/news/resources/press\\_kits/detail.jsp?pkid=ponemon-2013](http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013)  
• 9,839,450 x 188 = \$1,849,628,696

<sup>4</sup> 40% of SharePoint enterprises rely on Dropbox to share or sync documents while working on the go.  
• # of US businesses with 500+ employees: 18,469, representing 61,209,560 paid employees.  
<http://www.census.gov/econ/smallbus.html>  
• 58% of businesses with 500+ employees use SharePoint/Office 365, according to the study.  
(a potentially conservative estimate; industry stats for SharePoint use in enterprises are higher).  
• 66% use 2 or more computing devices, according to Forrester.  
• The ratio of white collar workers to the total worker population is 39%.  
<http://kff.org/other/state-indicator/blue-and-white-collar-workers/>.  
• 61,209,560 \* .58 \* .66 \* .39 = 9,138,097.63 white collar workers using redundant Dropbox licenses.  
• Assuming \$99/individual Dropbox license, that's \$904,671,666 spent on redundant licenses.

## What Is Keeping IT Professionals Up At Night?

It may surprise you that the most pervasive fear keeping IT professionals up at night is fear of accidental data meltdown. These events are terrifying because they're unintentional data compromises caused by sloppy employee practices, particularly mobile practices – and every company has mobile users.

Are all of YOUR mobile users always safe online?

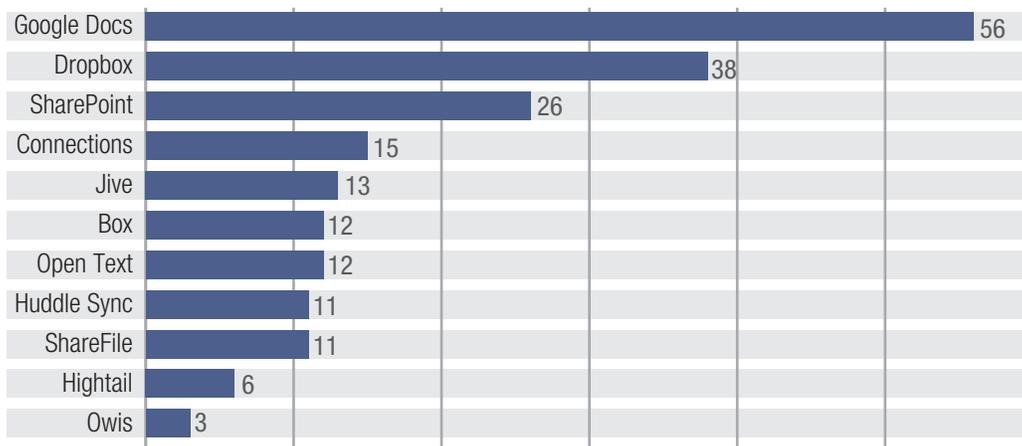
- The top three fears keeping IT professionals awake at night are: (select three of the list below, numbered 1, 2, 3 with one being the greatest fear.)

	1	2	3	Total
Fear of users losing devices	28 (34%)	26 (32%)	28 (34%)	82
Malware downloaded via third-party apps	25 (21%)	53 (45%)	39 (33%)	117
Viruses	39 (36%)	41 (38%)	27 (25%)	107
Data meltdown (loss of data), due to compromised documents lost via unsecure (unauthorized) file sync services	64 (50%)	21 (16%)	43 (34%)	128
Keeping pace with changing technologies	8 (14%)	24 (42%)	25 (44%)	57
Other	1 (25%)	0 (0%)	0 (75%)	4
<b>Total</b>	<b>165</b>	<b>165</b>	<b>165</b>	<b>495</b>

## Four in 10 Employees Ignore Their Company's IT Policy

In the past six months, 41% of mobile business users in the US have used an unsanctioned service such as Dropbox or Google Docs to share or sync docs on a mobile device.

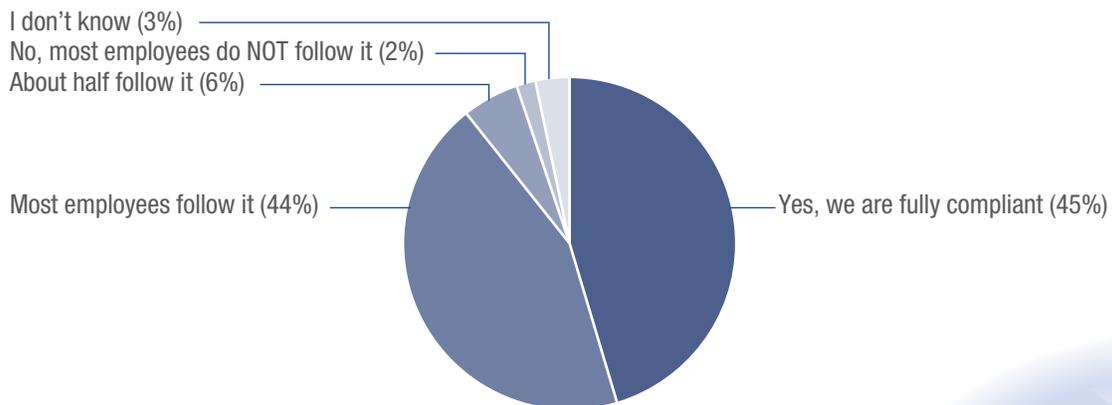
■ In the past six months I have used the following mobile apps to share or sync documents (select all that apply), notwithstanding the fact that enterprise IT has not specifically approved or subscribed to the service.



In the past six months, **41%** of mobile business users in the US have used an unsanctioned service such as Dropbox or Google Docs to share or sync docs on a mobile device.

This, despite **89%** saying all or most employees follow the company's document management policy.

■ Do employees follow your company's document policy?



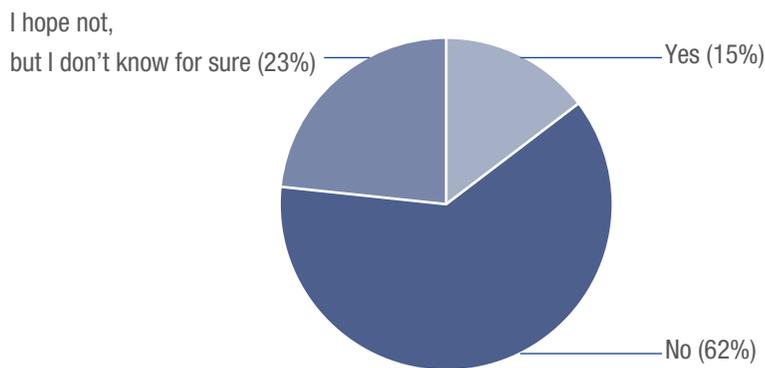
This **41%** translates into **14,937,553** rogue business users in the US, which is like saying every man, woman and child living in the greater Los Angeles metropolitan area is a rogue IT user.



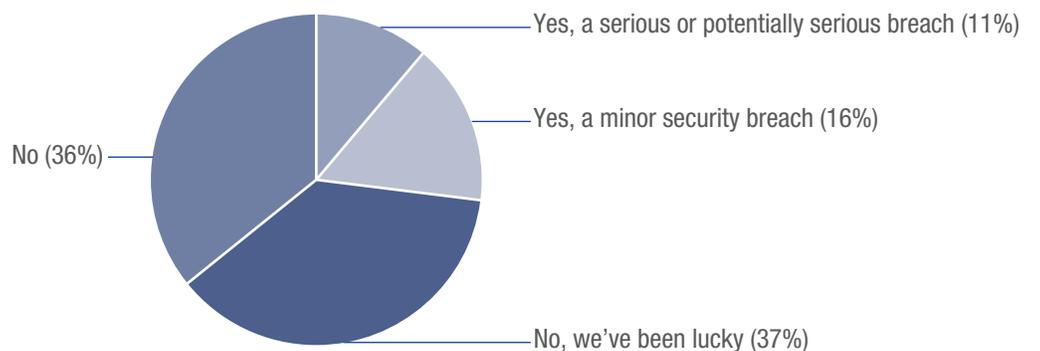
## More Than a Quarter of Business Users Admit to Causing a Security Breach

38% of respondents said that a document they shared using an unsanctioned service reached or may have reached an unintended recipient, and 27% of respondents confirmed that sharing a document this way caused a security breach.

- Have any of the documents shared (using services not specifically approved by your company) ever reached an unintended recipient?



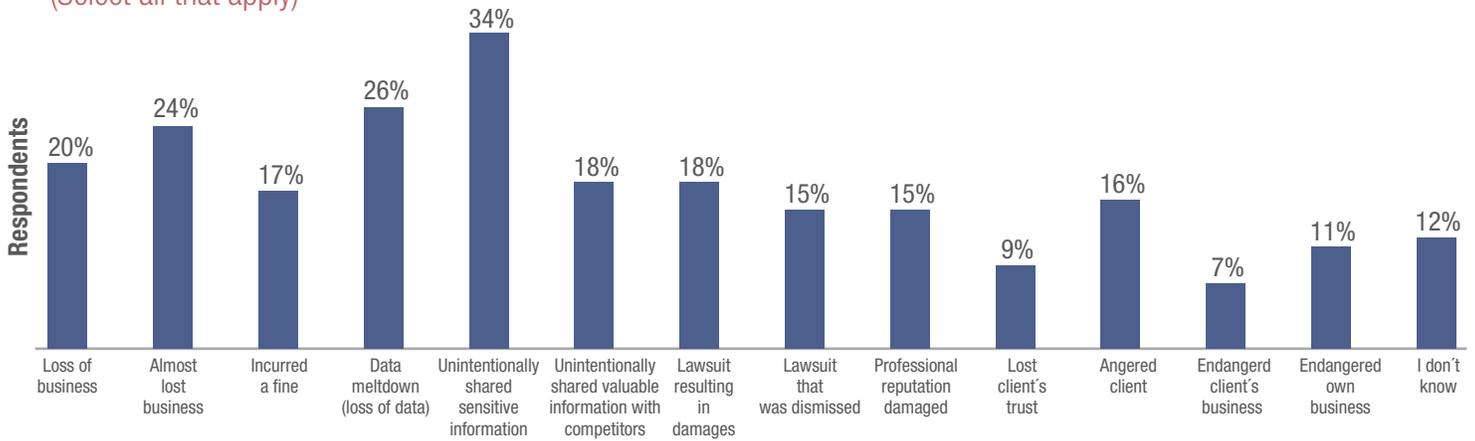
- Have you ever experienced a security breach when company documents were stored, synced, viewed, retrieved, emailed or edited using services that were NOT specifically approved by your company?



## The High Cost of Rogue IT

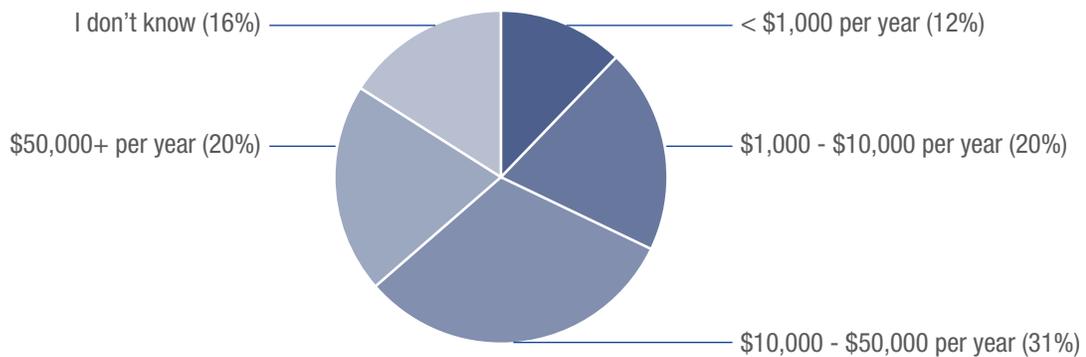
**One in four (27%) respondents** reported a negative business impact caused by a data leakage while sharing a document using an unsanctioned cloud service. The top three consequences reported: losing or nearly losing business; lawsuits resulting in damages, and unintentionally sharing sensitive information with a competitor.

- What consequences have you experienced when company documents were stored, synced, viewed, retrieved, emailed or edited using services that were NOT specifically approved by your company? (Select all that apply)



**Over half (51%) of those who reported a negative business impact** caused by sharing a document using an unsanctioned cloud service estimated the damages at more than \$10k per year and 20% estimated this damage at more than \$50K.

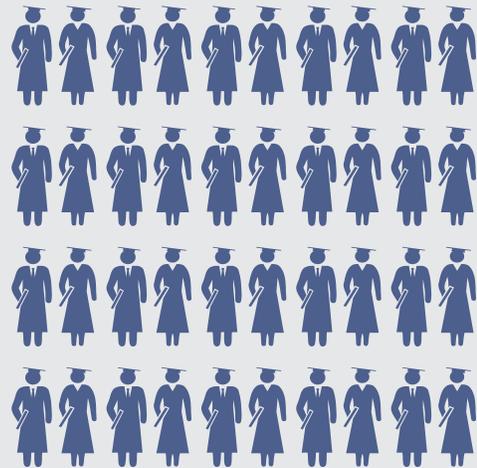
- How much did it cost to remedy situations that resulted when company documents were stored, synced, viewed, retrieved, emailed or edited (using services that were NOT specifically approved by my company)?



All told, the financial impact of data leakage resulting from handling company documents using unsanctioned services totals **\$1,849,628,696**. That's enough for the UN's World Food Program to feed **22 million undernourished children** a school meal for nearly a year<sup>5</sup> –and would certainly be money better spent!



In SharePoint organizations alone, businesses waste **\$904,671,666** by duplicating file sync/sharing services via Dropbox each year. This money could be better spent putting **40,639 students through one year of college**.



Adding insult to injury for Microsoft shops is an August 2013 security research report by Dhiru Kholia of Openwall and Przemysław Wegrzyn of CodePainters detailing various methods to bypass Dropbox's authentication, intercept SSL data and use a combination of code injection and 'monkey patching' techniques to hijack Dropbox accounts.<sup>6</sup>

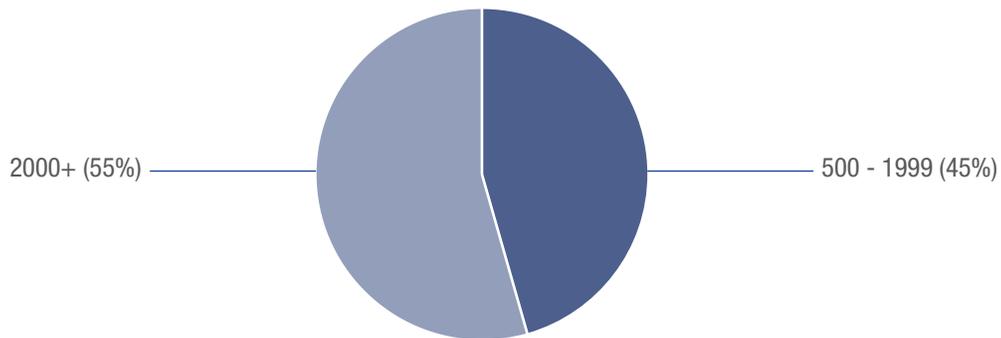
<sup>5</sup>  
1,849,628,696 x 4 25 cent meals per dollar = 7,398,514,784 meals  
• \$.25 = cost per school lunch (<http://walktheworldokc.blogspot.com/>)  
• 22 million: # of children the WFP feeds per day. Source: <http://www.wfp.org/school-meals>  
• 7,398,514,784 meals /22 million children = 336 days, which is the good part of a year

<sup>6</sup>  
• Average budget for in-state public college for the 2012–2013 academic year averaged \$22,261  
Source: [https://www.collegedata.com/cs/content/content\\_payarticle\\_tpl.jhtml?articleId=10064](https://www.collegedata.com/cs/content/content_payarticle_tpl.jhtml?articleId=10064)  
• \$904,671,666/\$22,261 = 40,639 students

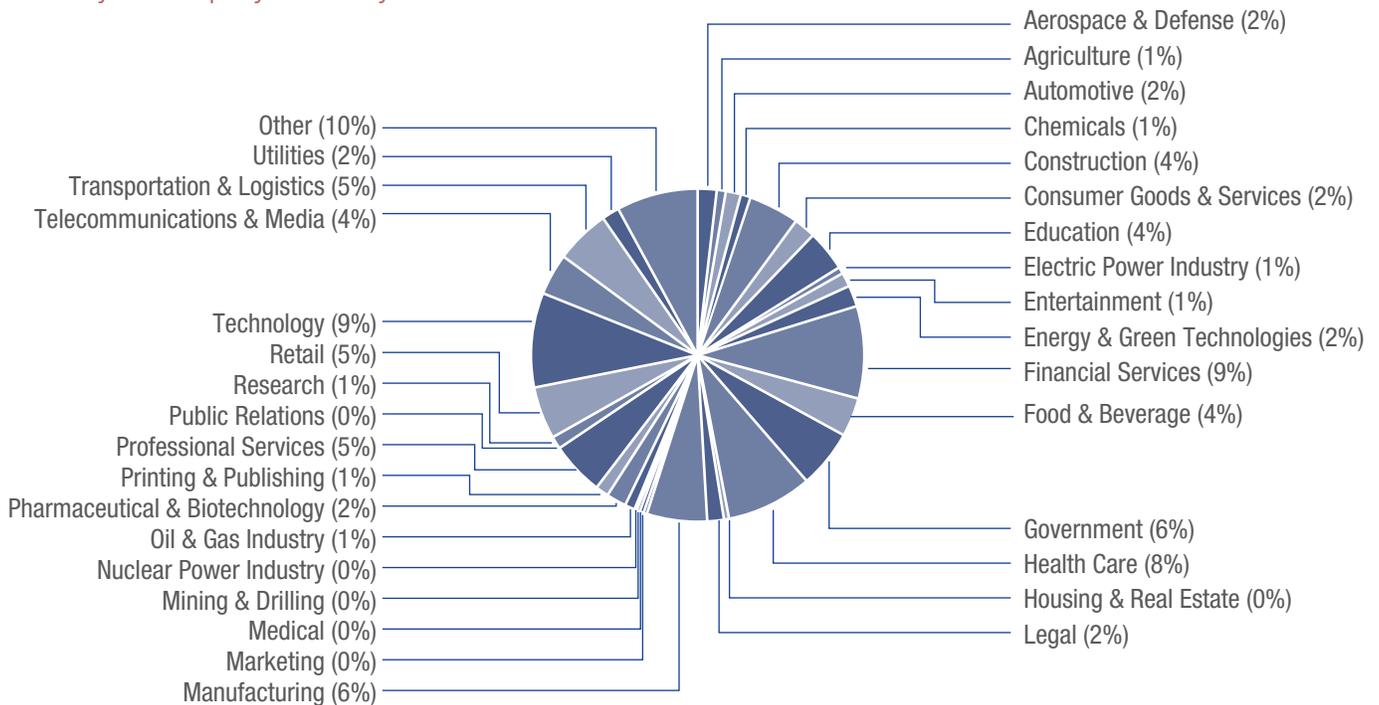
## Survey Demographics

Online market research firm uSamp fielded the survey on rogue IT practices August 13 – 27th, 2013 to 300 business IT users and 200 IT workers. Respondents use a tablet, smartphone or both to get work done; work in US and global businesses with 500+ employees, and are 20-64 years old. Margin of error is +/- 4.38 %.

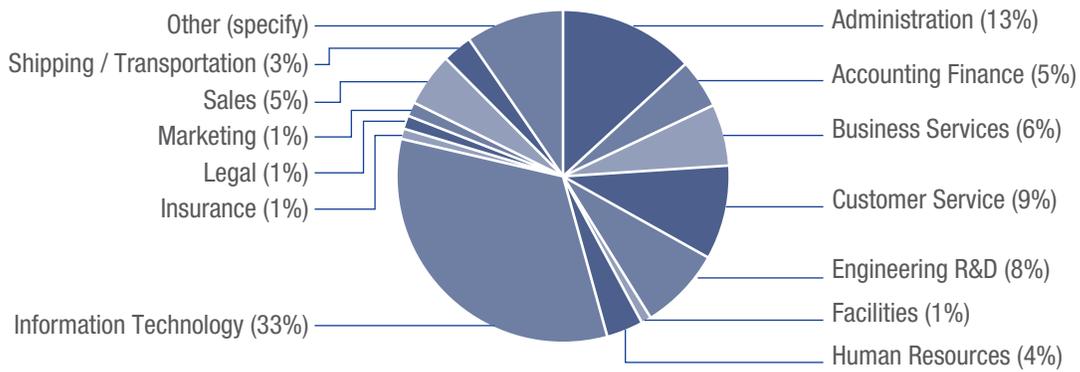
### ■ How many employees work at your current company?



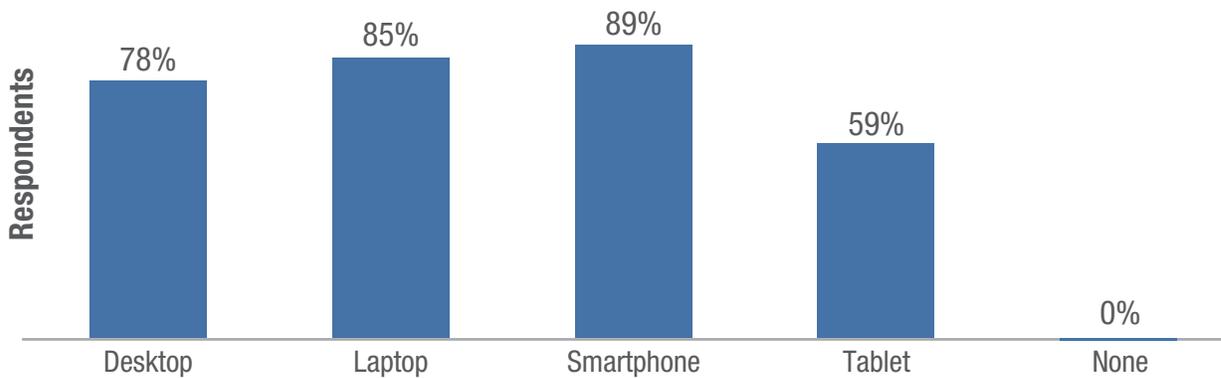
### ■ What is your company's industry?



■ What is your role within the company?



■ Which devices do you use to get work done?

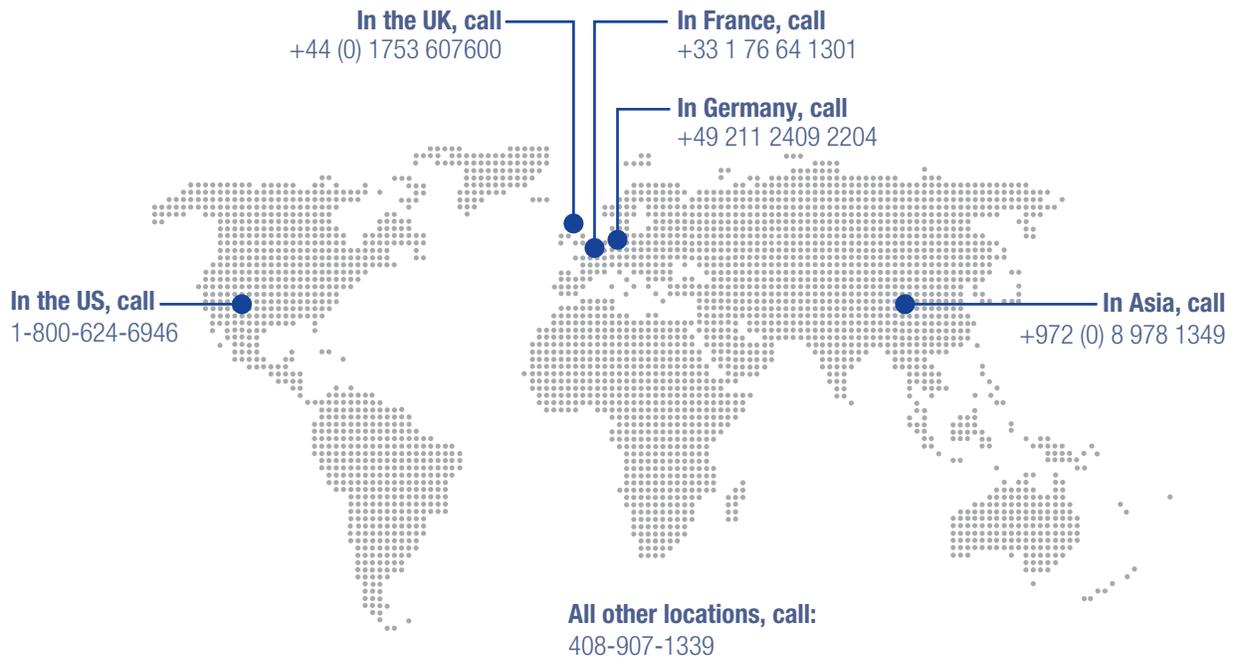


## About harmon.ie

harmon.ie (pronounced 'harmony') provides products for the mobile enterprise that deliver a consistent user experience on mobile devices, the desktop and the cloud for a host of social and collaboration platforms from vendors such as Microsoft and IBM. Thousands of businesses including Citi, DuPont and BAE Systems already use harmon.ie to empower their mobile workforce. For more information, visit <http://harmon.ie>.

## Contact Us

harmon.ie can help minimize rogue IT practices in your organization. We make enterprise document collaboration secure and social platforms easily accessible and drop-dead simple to use from any mobile device, desktop or the cloud. Please reach out to us at one of the following contact points:



 [www.facebook.com/teamharmonie](http://www.facebook.com/teamharmonie)

 [www.linkedin.com/company/harmon.ie](http://www.linkedin.com/company/harmon.ie)

 [www.youtube.com/user/TeamHarmonie](http://www.youtube.com/user/TeamHarmonie)

 Twitter @TeamHarmonie

 Email [info@harmon.ie](mailto:info@harmon.ie)

 [www.harmon.ie](http://www.harmon.ie)