Shadow IT is real: 1 in 2 employees use unauthorized file services in order to get their job done.

Thea Ulimoen, Anita Eriksen, Jacopo Paglia, Kai Roer[1]

Abstract

"The use of unauthorized cloud services and file sharing services is known to increase security risks as documents can bypass controls put in place by organisations. Understanding how common it is for employees to bypass security controls is a measurement of security behavior and is directly linked to security culture. In this report we examine the prevalence of two common insecure practices using survey responses across global regions and industries. The first analysis examines the use of unauthorized cloud services to store information and communicate in the workplace. In the second analysis we examine the prevalence of downloading content through unauthorized file sharing networks using work computers. Our results demonstrate that an alarmingly high percentage of employees report the use of unauthorized cloud services and file sharing services at their workplace. The use of unauthorized file sharing networks in the workplace is most prevalent in Asia, with over 50\% of respondents stating that this is normal practice in their organisation, which is in stark contrast to Africa with a comparatively smaller 19.6\%. When examining the practices by industry sector, we document a large disparity between different industries. Our data demonstrates the degree of variation in unsecure practices across regions and industries. They also highlight that even for regions and industries who report the lowest rates of insecure practices, almost one in five employees report that such behaviors are normal in their organization."

1.research@knowbe4.com

Method

This report made use of items selected from the Security Culture Survey, which is available to KnowBe4 customers via the Kevin Mitnick Security Awareness Training (KMSAT) platform. The Security Culture Survey was developed by CLTRe (now KnowBe4 Research) based on a scientific approach that integrates survey methodology, statistics, and scientific findings from security culture research and psychometrics (Security Culture Report, 2017, CLTRe). The survey consists of statements designed to assess different aspects of security culture, during which respondents answer questions using a 5-point Likert scale. Two questions were selected for analysis pertaining to the following common security related behaviors:

Behavior 1 - perceived prevalence of use of unauthorized cloud services within the organisation.

Behavior 2 - perceived prevalence of use of unauthorized file-sharing networks to download content via work computers.

Raw responses for these questions were collected and then re-coded for the purpose of analysis, whereby positive and negative responses were assigned the values 'yes' or 'no' respectively. A total of N = 435 395 respondents were included in the analysis. For the purposes of comparison, respondents were grouped by industry type (Banking, Financial Services, Technology, Education, Construction, Government, Manufacturing, Insurance, Consulting, Business Services, Consumer Services, Not for Profit, Healthcare & Pharmaceuticals, Transportation, Legal, Retail & Wholesale and Energy and Utilities) and global region (Africa, Asia, Europe, Latin America, North America, Oceania). The data for this report is aggregated from a single data collection time point for each employee, collected in July of 2021. Participants were informed that their responses were anonymous prior to completing the survey.

Results

Behavior 1 - *Perceived prevalence of use of unauthorized cloud services within the organisation.*

An overview of results for responses to behavior 1 from the best and worst performing industries can be viewed in Table 1. A comprehensive overview of regional data can be found in Table 2. The data reveals significant variation between regions. Respondents

Best	N	Yes	No
Banking	35 459	17.7%	82.3%
Financial services	30 428	20.5%	79.5%
Technology	54 253	21.3%	78.7%
Worst			
Government	28 476	33.4%	66.6%
Construction	6 207	35.5%	64.5%
Education	6 444	42.8%	57.2%

Table 1: Summary of responses for the best and worst performing industries regarding whether it is common practice for employees to use unauthorized cloud services at work.

Region	N	Yes	No
Latin America	1 314	20.4%	79.6%
Africa	28 000	20.5%	79.5%
Europe	29 582	24.8%	75.2%
North America	234 887	27.0 %	73.0%
Oceania	7 281	32.0%	68.0%
Asia	3 943	32.6%	67.4%

Table 2: Summary of responses by global region regarding whether it is common practice for employees to use unauthorized cloud services at work.

from Oceania (32.0%) and Asia (32.6%) have the highest rate of reporting unauthorized cloud services as normal practice at their organisations, constituting the highest rate of use of all regions examined. In contrast, Africa (20.5%) and Latin America (20.4%) have the fewest respondents reporting this as normal practice. Respondents from organizations in Europe (24.8%) and North America (27.0%) perform equitably, with both regions falling in the mid-range of those examined.

A comparison of responses to behavior 1 by industry revealed the lowest reports of this practice were from employees associated with banking (17.7%), financial services (20.5%), and technology (21.3%). The highest percentages, and thus worst performing in terms of security, were from industries within government (33.4%), construction (35.5%) and education (42.8%).

Behavior 2 - *Perceived prevalence of use of unauthorized file-sharing networks to download content via work computers.*

An overview of results for the best and worst performing industries in response to behavior 2 can be viewed in Table 3, while a comprehensive regional overview is available in Table 4. The percentage of respondents who report that downloading content through unauthorized file-sharing networks is a com-

Best	N	Yes	No
Banking	43 061	18.5%	81.5%
Insurance	16 977	23.1%	76.9%
Financial services	38 262	23.4%	76.6%
Worst			
Manufacturing	32 808	35.0%	65.0%
Education	11 274	38.5%	61.5%
Construction	9 629	41.0%	59.0%

Table 3: Summary of responses for best and worst performing industries regarding whether employees use their computers to download content through file sharing networks

Region	N	Yes	No
Africa	28 000	19.6%	80.4%
Latin America	1 314	25.6%	74.4%
Europe	29 582	29.0%	70.0%
North America	234 887	29.6 %	70.4%
Oceania	7 281	30.6%	69.4%
Asia	3 943	54.6%	45.4%

Table 4: Summary of responses by global region regarding whether employees use their computers to download content through file sharing networks

Figure 1: An overview of the percentage of respondents who agreed that is was common practice within their organisation for employees to use unauthorized cloud sharing services. A larger scale version of this map is available in the appendices.

Figure 2: An overview of the percentage of respondents who agreed that is was common practice within their organisation for employees to use file sharing services. A larger scale version of this map is available in the appendices.

mon practice within their organisation was highest throughout Asia (54.6%). The difference in percentage for the following 4 highest reporting are minimal with Latin America (25.6%), Europe (29%), North America (29.6%) and Oceania (30.6%) producing similar outcomes. The lowest rate of reporting use of unauthorized file sharing networks as normal practice came from employees in Africa (19.6%).

There is also variability in outcomes between industry types, with those providing banking (18.5%), insurance (23.1%) or other financial services (23.4%) demonstrating the lowest percentages of individuals who perceive this as common practice within their organization. In contrast, manufacturing (35%), education (38.5%) and construction (41%) industries had the highest percentage.

Discussion

The data presented here offers insight into the prevalence of two common insecure practices across regions and industry. Organisations from Africa consistently demonstrate the safest performance of regions analysed through the lowest percentages reporting the behaviors, while Asia and Oceania are both regions who report consistently higher risk percentages (see Figure 1 and 2). While the majority of regions 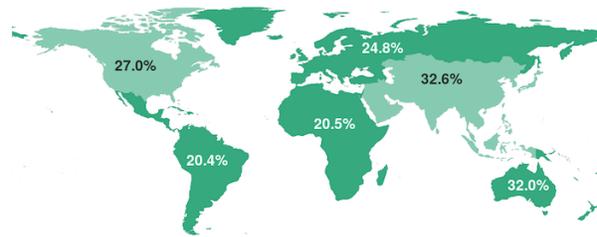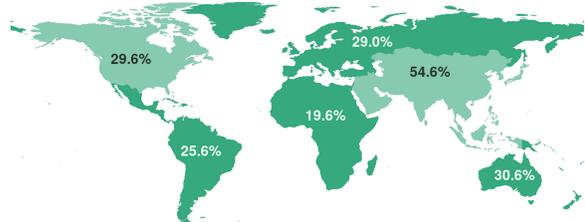display similar percentages for both practices, Asia in particular presents a large difference between the two, with 22% more respondents reporting common use of content through file sharing networks compared with use of unauthorized cloud usage. This suggests that actions towards preventing the practice of file sharing ought to be prioritized for this region, for example by improving training and communication on the risks involved when using unauthorized cloud and file sharing services.

There is a notable consistency across industries in the prevalence of both practices. Both education and construction are among the highest percentages responding yes both to knowing others who download content through file sharing networks, and reporting the use of unauthorized cloud services as the norm in their organisations. A similar pattern can be seen with the best performing industries, with both banking and financial services being the lowest reporting for both practices. This consistency highlights the importance of assessing different aspects of security culture, and assessing whether certain norms, behaviors or attitudes may be contributing to the normalization and active use of other unsafe practices.

Implications

There are a number of stand out findings from the report. One of the more extreme findings is that of those surveyed in Asia, over 50% report that use of unauthorized file sharing networks on company computers is a common practice at their organisation. This is likely driven by a number of causes, however one area of particular interest is the unique and varied landscape of attitudes and laws towards file sharing networks across Asia. This result may be partly driven by the lack of availability of legal methods for downloading digital content in a number of Asian countries, which appears to encourage people to use file sharing sites for media downloads. For example, consumers in Singapore have cited a lack of legal media content availability as a reason why they believe using file sharing networks to download copyrighted content is OK. One report suggests that as many as 1 in 2 are in support of their use (Asia One publication, April 24th 2015 "One in 2 here OK with illegal file-sharing"), a number of interest here given our findings show that 1 in 2 from the Asia region report using unauthorized file sharing networks at work as normal practice. While it may not be immediately clear how this would affect work environments directly, regular use in home environments as well as generally positive attitudes towards their use is likely to wear down inhibitions to using file sharing networks at work, especially if the employee feels this method offers enough benefits such as saving time or convenience.

Another finding of particular interest is the consistent positive outcomes from the African region across both assessed practices. This could be due to the delay in IT development within the region that has allowed organisations in Africa access to knowledge and understanding of cyber threats other regions have had to learn through experience. South Africa is also a leading producer of scientific research into the human factors of cyber based social engineering (e.g. see relevant works of B. Van Niekerk, J. Van Niekerk, Reid, Von Solms, Da Veiga, Ramluckan), since as early as 2009. It is likely that this knowledge and prioritization of research is contributing to good practice among organisations within the country, influencing the Africa region data.

North America and Europe appeared in the middle rankings consistently. Neither of these regions have shown percentages consistent with secure behavior, and organisations in both regions should consider taking steps towards both assessing and preventing future occurrences of use of unauthorized cloud services and file sharing services.

The findings from the industry analysis are consistent with findings from our previous reports (Security Culture Report 2017, 2020, 2021) where finance and technology based organisations produce outcomes reflecting safer practice than many other industries (see Tables 5 and 6 for a comprehensive overview of all industries considered). This is unsurprising given the high value of financial data, which typically translates to government mandated training and a strong drive to understand and mitigate risk, while technology-based organisations typically have employees who have significant knowledge of cyber space and are reliant on keeping their computer systems safe. While these industries have performed well relative to the comparative analysis, there are still upwards of 19% of respondents reporting use of unauthorized cloud services and file sharing services as normal practice. So while these appear to be less vulnerable than others, they are still not invulnerable and should take necessary steps to assess the extent of this behavior in organisations and address them through relevant training or policy implementation.

Similarly, outcomes for previous assessments of security culture have cited construction and education as two of the worst performing industries, a finding that is also reflected here. Previous analyses have identified a lack of knowledge in the construction as being a primary cause of consistently risky outcomes, and it is probable that this is continuing to contribute to the industries' poor performance here. Education, government and manufacturing have all scored poorly on reports of both practices and should urgently reconsider their approaches and efforts to disseminate and train good security practices in individual organisations.

Conclusion

This report demonstrates that no region or industry prevents risky use of unauthorized cloud services or file sharing services in the workplace to such a degree as to be confident of no security breaches via these methods. Asia and Oceania are regions with worryingly high rates of both practices, while Africa is consistently the best performing. Finance and technology based industries are comparatively better than many other industries, while construction, manufacturing, educational and government based organisations are the poorest performing. While the worst performing industries and regions presented here should consider immediate action in the form of assessment and implementation of policy and training, with prioritisation based on analysis, even those with the best performance have a rate of 1 in 5 employees engaging in this behavior. All industries and regions should

4

consider methods of preventing future engagement of these behaviors within organisations.

About KnowBe4, Inc.

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 34,000 organizations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security. Kevin Mitnick, an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as the last line of defense.

About the KnowBe4 Research Technical Report

Establishing an excellent security culture is an important aspect of developing an efficient defense against cyber security threats. Reports from KnowBe4 Research provide analysis of various aspects of security culture, in order to provide quantifiable, up to date information about global practices and standards in different industries.

About KnowBe4 Research

KnowBe4 Research is the research arm of KnowBe4, Inc. Our mission is to provide IT and security leaders with high quality, vendor neutral data-driven insights related to cybersecurity and the human element.

References

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207.

Da Veiga, A., Ochola, E., Mujinga, M., Padayachee, K., Mwim, E., Kritzinger, E., ... & Machaka, P. (2021, July). A Reference Point for Designing a Cybersecurity Curriculum for Universities. In International Symposium on Human Aspects of Information Security and Assurance (pp. 46-62). Springer, Cham.

Gcaza, N., & Von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. The Electronic Journal of Information Systems in Developing Countries, 80(1), 1-17.

Ramluckan, T., van Niekerk, B., & Leenen, L. (2019, July). Research challenges for cybersecurity and cyberwarfare: A South African perspective. In Proceedings of the 18th European Conference on Cyber Warfare and Security (pp. 372-378).

Reid, R., & Van Niekerk, J. (2014, August). From information security to cyber security cultures. In 2014 Information Security for South Africa (pp. 1-7). IEEE.

Reid, R., & Van Niekerk, J. (2014). Towards an Education Campaign for Fostering a Societal, Cyber Security Culture. In HAISA (pp. 174-184).

Reid, R., Van Niekerk, J., & Von Solms, R. (2011, August). Guidelines for the creation of brain-compatible cyber security educational material in Moodle 2.0. In 2011 Information Security for South Africa (pp. 1-8). IEEE.

Gcaza, N., & Von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. The Electronic Journal of Information Systems in Developing Countries, 80(1), 1-17.

van Niekerk, B., & Ramluckan, T. (2019, July). A Legal Perspective of the Cyber Security Dilemma. In European Conference on Cyber Warfare and Security (pp. 544-XX). Academic Conferences International Limited.

Appendices

The appendices attached here offer visualizations and detailed overviews of the data described in the report.

Appendix A includes data for the prevalance of use of unauthorized file sharing networks at work.
Appendix B includes data for the prevalence of use of unauthorized cloud sharing services at work.
Appendix C includes supplementary data. Here you will find the list of countries included in the regional analysis.
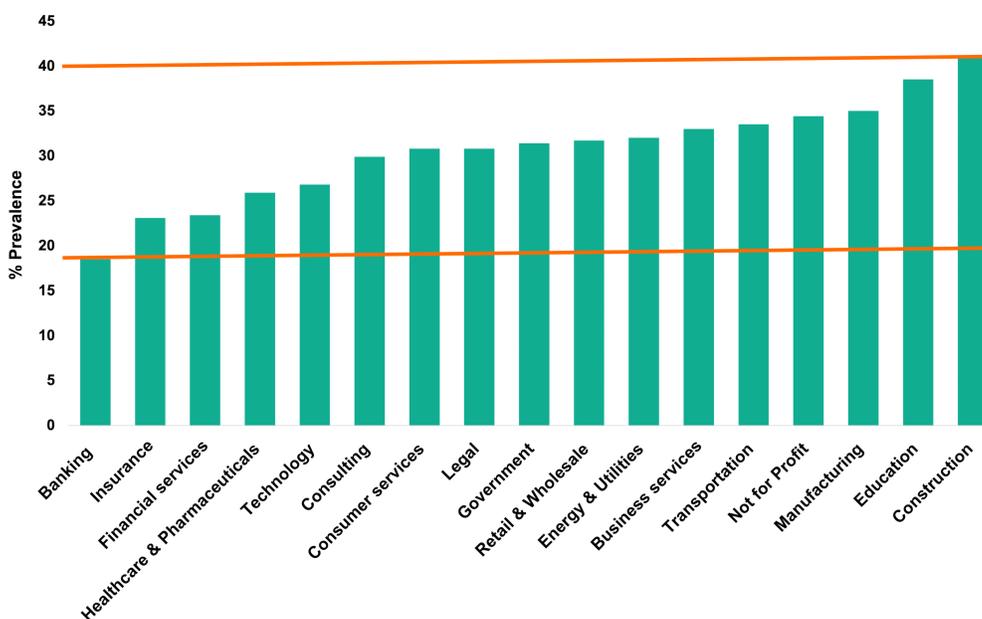
Appendix A

Reported rate of perceived use of unauthorized file sharing networks

Results by industry:

Reported rate of perceived use of unauthorized file sharing networks at work by industry, ranked from best to worst:
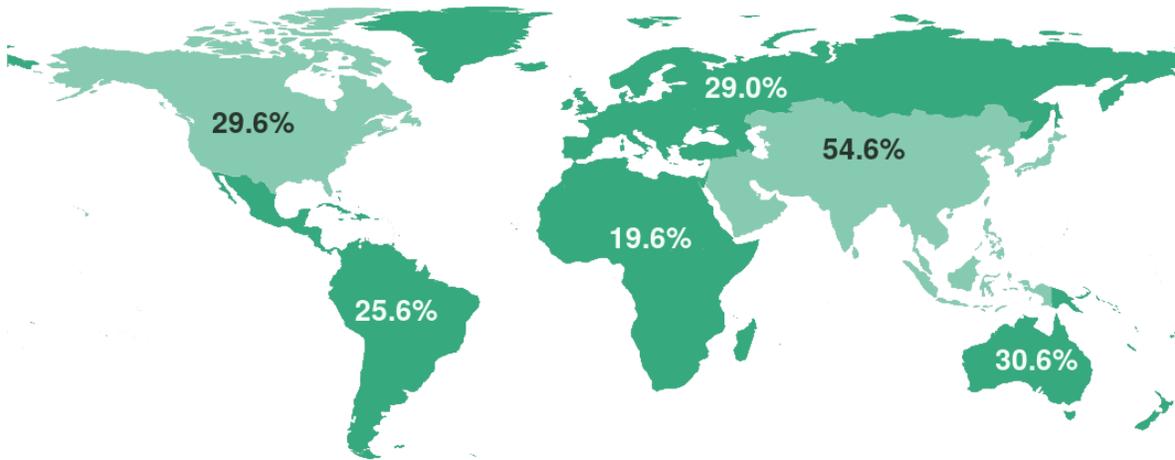
Industry type	N	Yes (%)	No (%)	Rank
Banking	43 061	18.5	81.5	1st
Insurance	16 977	23.1	76.9	2nd
Financial services	38 262	23.4	76.6	3rd
Healthcare & Pharmaceuticals	26 306	25.9	74.1	4th
Technology	68 954	26.8	73.2	5th
Consulting	13 567	29.9	70.1	6th
Consumer services	6 578	30.8	69.2	7th
Legal	2 805	30.8	69.2	7th
Government	42 788	31.4	68.6	9th
Retail & Wholesale	28 613	31.7	68.3	10th
Energy & utilities	13 404	32.0	68.0	11th
Business services	13 008	33.0	67.0	12th
Transportation	12 393	33.5	66.5	13th
Not for Profit	16 540	34.4	65.6	14th
Manufacturing	32 808	35.0	65.0	15th
Education	11 274	38.5	61.5	16th
Construction	9 629	41.0	59.0	17th

A graphical overview of perceived use of unauthorized file sharing networks at work by industry:

Results by global region:

An overview of the percentage of respondents who agreed that is was common practice within their organisation for employees to use file sharing services

Summary of responses by global region regarding whether employees use their computers to download content through file sharing services

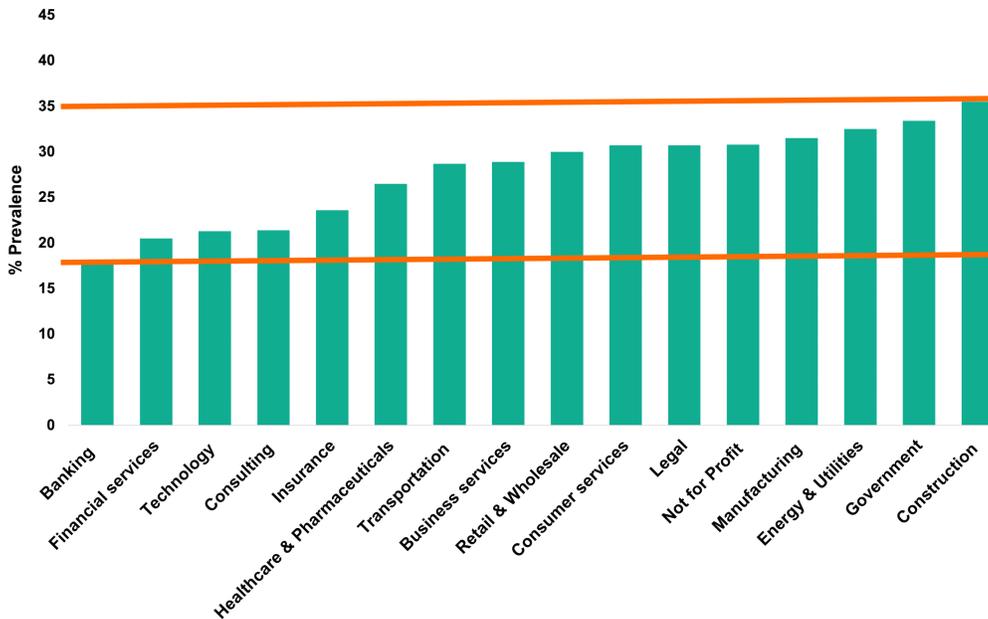| Region	N	Yes	No	Rank
Africa	28 000	19.6%	80.4%	1st
Latin America	1 314	25.6%	74.4%	2nd
Europe	29 582	29.0%	70.0%	3rd
North America	234 887	29.6 %	70.4%	4th
Oceania	7 281	30.6%	69.4%	5th
Asia	3 943	54.6%	45.4%	6th

Appendix B

Reported rate of the perceived use of unauthorized cloud services at work

Results by industry:

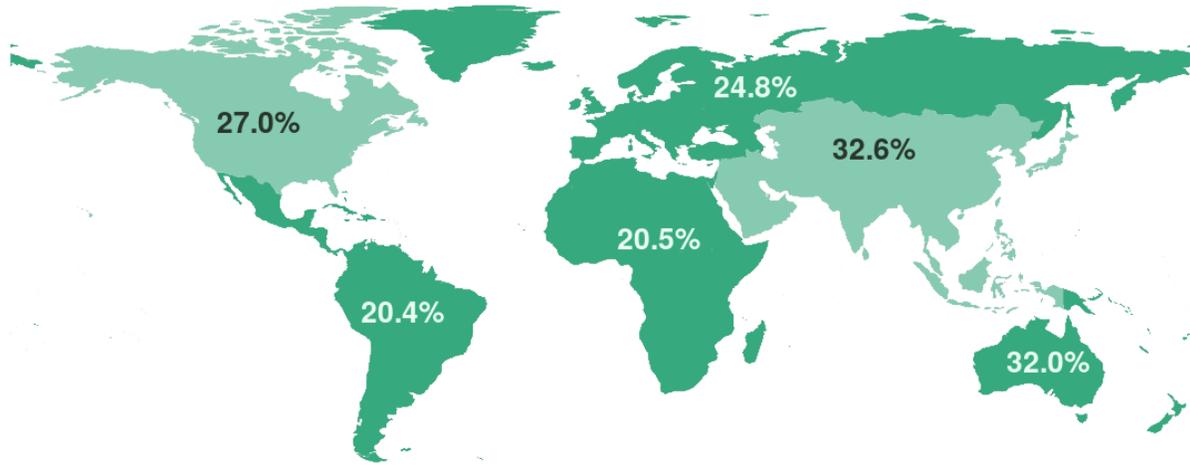**Reported rate of the perceived use of unauthorized cloud services at work by industry, ranked from best to worst:**

Industry type	N	Yes (%)	No (%)	Rank
Banking	43 061	17.7	82.3	1st
Financial services	38 262	20.5	79.5	2nd
Technology	68 954	21.3	78.7	3rd
Consulting	13 567	21.4	78.6	4th
Insurance	16 977	23.6	76.4	5th
Healthcare & Pharmaceuticals	26 306	26.5	73.5	6th
Transportation	12 393	28.7	71.3	7th
Business services	13 008	28.9	71.1	8th
Retail & Wholesale	28 613	30.0	70.0	9th
Consumer services	6 578	30.7	69.3	10th
Legal	2 805	30.7	69.3	10th
Not for Profit	16 540	30.8	69.2	12th
Manufacturing	32 808	31.5	68.5	13th
Energy & utilities	13 404	32.5	67.5	14th
Government	42 788	33.4	66.6	15th
Construction	9 629	35.5	64.5	16th
Education	11 274	42.8	57.2	17th

A graphical overview of the perceived use of unauthorized cloud services at work by industry

Results by global region:

An overview of the percentage of respondents who agreed that is was common practice within their organisation for employees to use unauthorized cloud sharing services by region.

Summary of responses by global region regarding whether it is common practice for employees to use unauthorized cloud services at work.

Region	N	Yes	No	Rank
Latin America	1 314	20.4%	79.6%	1st
Africa	28 000	20.5%	79.5%	2nd
Europe	29 582	24.8%	75.2%	3rd
North America	234 887	27.0 %	73.0%	4th
Oceania	7 281	32.0%	68.0%	5th
Asia	3 943	32.6%	67.4%	6th

Appendix C

Countries included in regions for analyses:

Region	Countries Included
Asia	Singapore | Hong Kong | India
	Malaysia | Philippines
Oceania	Australia | Indonesia | New Zealand
North America	United States of America | Canada
	Barbados | Bermuda | Bahamas
Europe	Netherlands | Sweden | Belgium | France
	Finland | Greece | Cyrpus | Gibraltar | Norway
	Ireland | Luxembourg | Malta | Denmark
	Austria | Portugal | Lithuania | Spain
	Germany | Italy | United Kingdom | Switzerland
Latin America	Brazil | Grenada | Saint Kitts and Nevis
	Ecuador | Belize | Trinidad and Tobago
	Jamaica | Guatelmala | Suriname
	St Maarten | Mexico | Panama
Africa	South Africa | Kenya | Botswana
	Ghana | Mauritius | Mozambique | Zambia
	Rwanda | Uganda | Zimbabwe | Eswatini
	Nigeria | Rep. of Tanzania | Namibia