



2014 Danger in the Cloud Report

Tresorit research report: examining the attitudes on the safety and security of professional and private information online in the U.S.

September 2014

Foreword by Istvan Lam, CEO, Tresorit

The issue of online security has never been more prevalent in public dialogue. Americans are increasingly aware of widespread government surveillance programs that repeatedly break public trust in the name of national security. Hackers dominate headlines by hatching data breaches that result in staggering costs—both financially and in customer confidence.

But has any of this convinced Americans to take charge of their own digital security?

Released this past May, Part I of our research, which was conducted by YouGov, showed that more than half of employed Americans thought Snowden was right to reveal the massive dragnet utilized by the National Security Agency. In the wake of these findings on perceptions towards cyber security and privacy, we wanted to uncover how Americans are acting on their beliefs today. Alarmingly, our new study reveals that 37 percent of employed Americans have not done anything to protect themselves online and that nearly half of employed Americans today do not trust cloud storage and sharing platforms. Yet, despite these findings, 27 percent would upload corporate data without even thinking twice about the consequences.

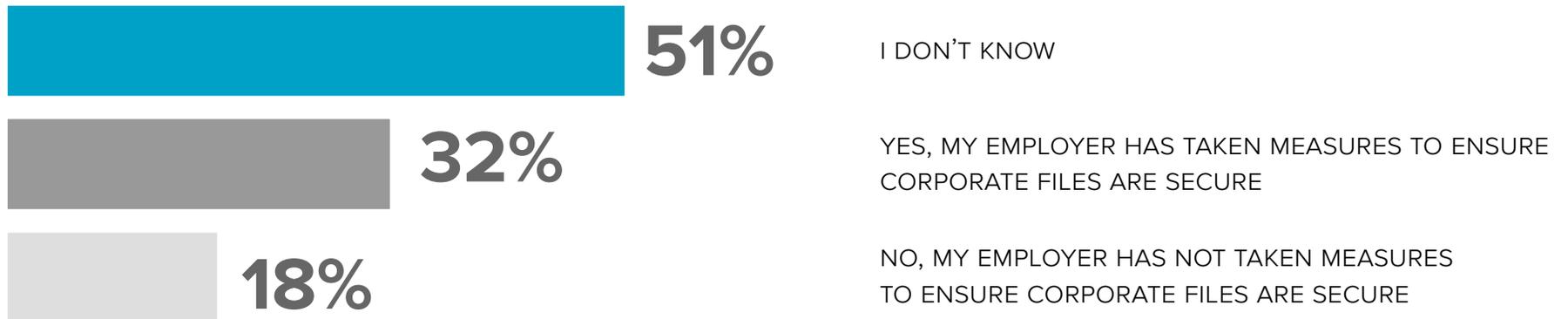
Following these results, our research shows that Americans today are keen to protecting themselves and their data online, but are simply unaware of the various solutions available to them. This lack of awareness, ultimately, results in data stored online under a false sense of security. Additionally, our research further demonstrates that American businesses are not educating employees well enough on the security measures that protect their corporate data.

This is why Tresorit exists. More than a year after the Snowden leaks and major corporate data breaches, the need for an easy-to-use, secure storage and sharing platform is at an all-time high. Through our end-to-end encrypted cloud service, we allow businesses and individuals alike to protect their data against the emerging threats of hackers and widespread, unwarranted surveillance.

Istvan Lam
CEO, Tresorit
www.tresorit.com



Has your employer taken any measure to ensure corporate files are secure?



A bit more than half of the respondents say they are “not sure” if their company has taken any security measures. Responsibility for such confusion rests firmly on the company’s shoulders: you can’t expect employees to adhere to a policy that they are not aware of.

You mentioned that your employer has taken security measures to ensure corporate files are secure.

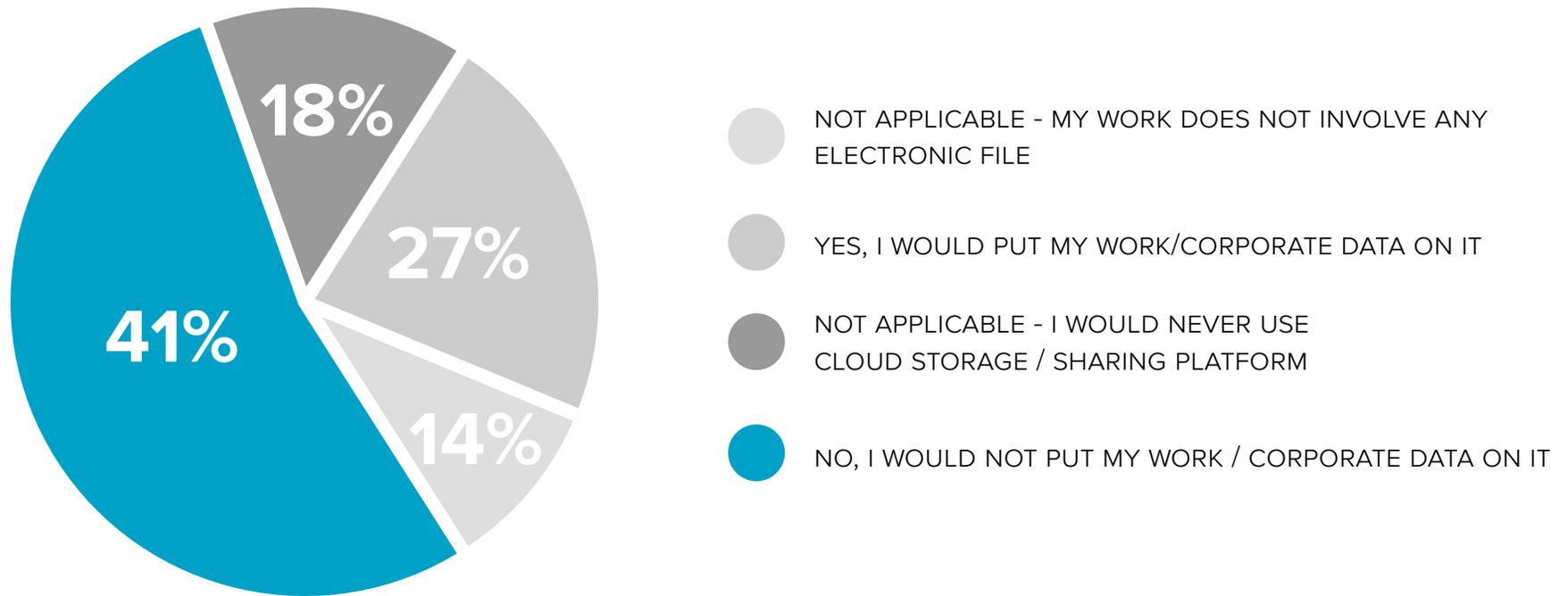
In which of the following ways has that impacted your work, if any? (Check all that apply.)



On the other hand complying with company policies can decrease work efficiency (according to 14% of respondents) and 10% even said that they have tried to circumvent security measures to get their job done. As it turns out users overwhelmingly turn to non-approved apps or IT solutions for one reason: they need to get their jobs done, and that's simply not possible with current security solutions.

Imagine you are using cloud storage and sharing platforms for personal use.

Would you put your work/corporate data on it?



The cloud is partly responsible for the rise of shadow IT in business. As almost the third of the respondents said that they would store business documents in their private cloud accounts, trying to limit usage of cloud storage in your business is like shutting the barn door after the horse has escaped: it won't help. Instead, choose cloud services that provide advanced data control options. This enables your employees to do their jobs the way they want to, without compromising company security and liability.

Even if your company does not, imagine you are using cloud storage and sharing platforms at work.

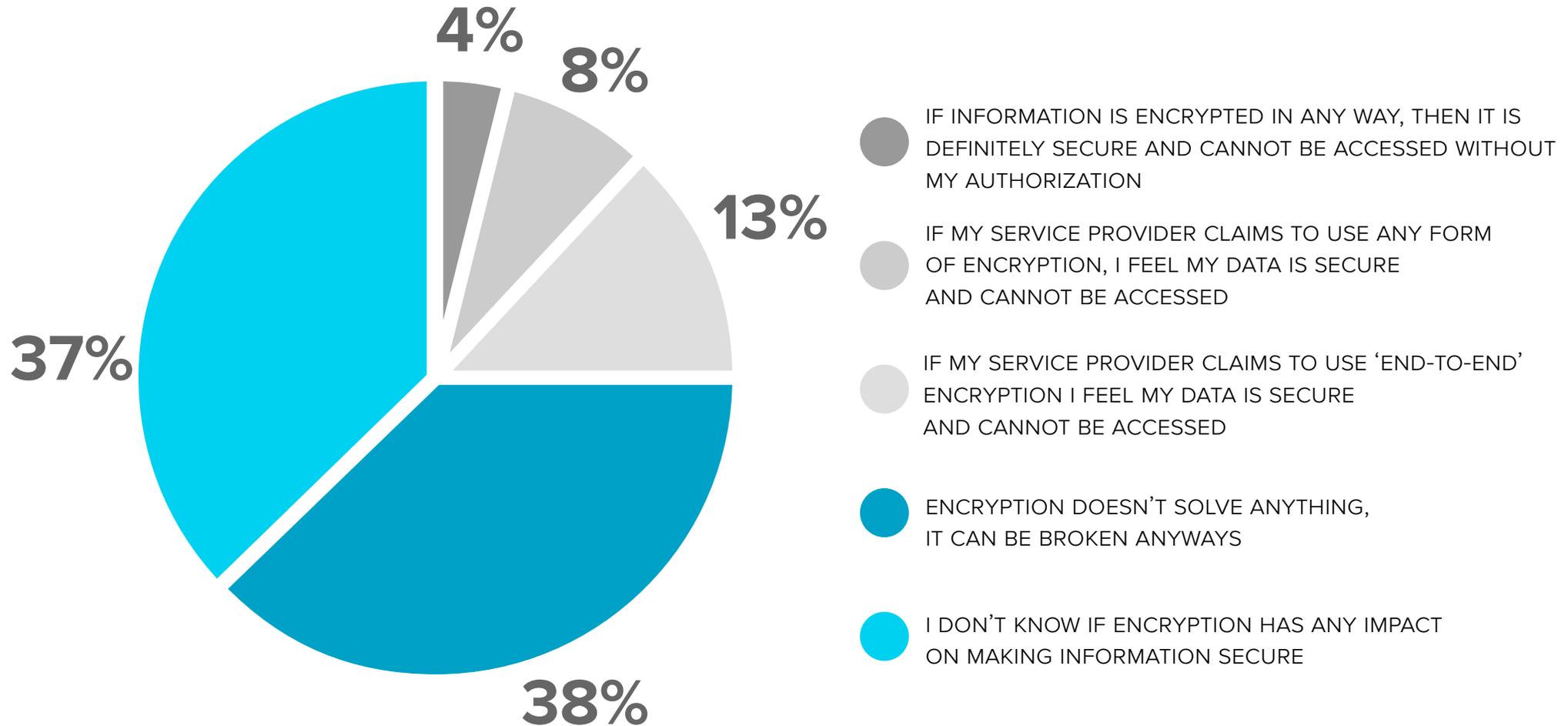
Would you feel that your information, files and content are secure?



Employee's confusion about the cloud shows that without properly training people using the technology, organizations will be exposed to tremendous risk. You can see that although a third would put data on the cloud, almost half do not trust the cloud at all.

Encryption is a process of securing information online, essentially using an electronic lock and key system for data.

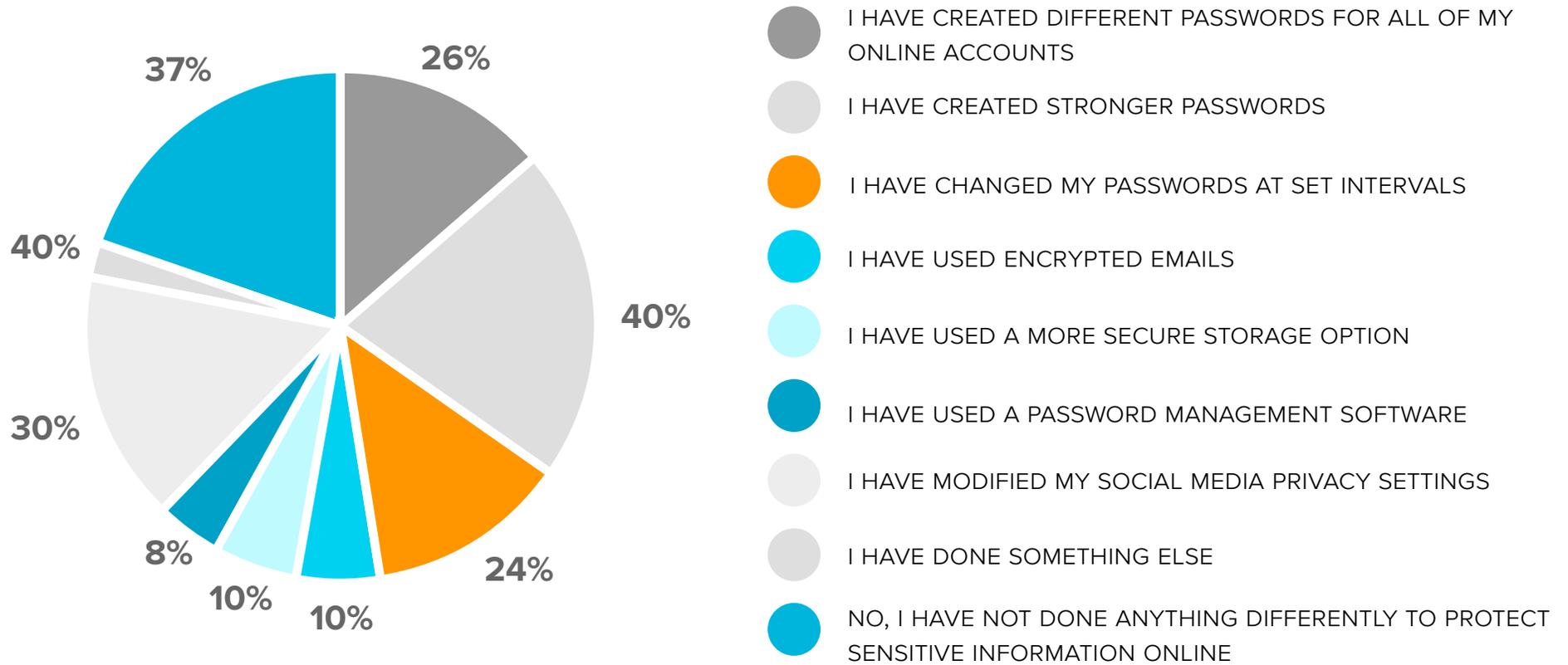
Which of the following statements describes your view of the security achieved by encryption?



More than one in three (37%) Americans do not know if encryption has an impact on making online information secure and 38 percent feel encryption does not solve any problems, and that it can be broken show that Americans are also oblivious to the capabilities of encryption. Only 13 percent are aware of the importance of service providers can only create zero knowledge environment by using “end-to-end” encryption.

Edward Snowden exposed the National Security Administration's (NSAs) PRISM surveillance data program in which the US government accessed citizen's private search data and other Internet traffic without the permission or knowledge of those affected.

In that time, have you done any of the following to protect sensitive information online?



Password protection is not enough: however 40 percent have created stronger passwords; as the number of online security breaches has grown steadily, passwords alone are feeble security measures. Only a select few enact true security solutions: while only 10 percent of Americans have used encrypted emails, 10 percent have also used a more secure storage option, and a startlingly low 8 percent have used password management software. Are people lazy when it comes to online security?

Research Methodology

Total sample size was 1007 adults. Fieldwork was undertaken between 19 - 21 May 2014. The survey was carried out online. The figures have been weighted and are representative of all US employees (aged 18+).

About Tresorit

Built from the ground up to withstand today's most sophisticated cyber-attacks and data leaks, Tresorit offers the most complete secure workflow in the cloud. Using patented encryption technology, Tresorit is answering the demand for modern collaboration solutions with built-in, end-to-end encryption for document-centric security. Leveraging a simple, easy to use end-user interface, Tresorit is ideal for small and medium enterprises who need compliance, control and confidentiality, as well as collaboration and backup.

Tresorit is available for [Windows](#), [Mac](#), [Android](#), [iOS](#), [Windows Phone](#) and [BlackBerry](#).

For more information and to download Tresorit, visit www.tresorit.com.