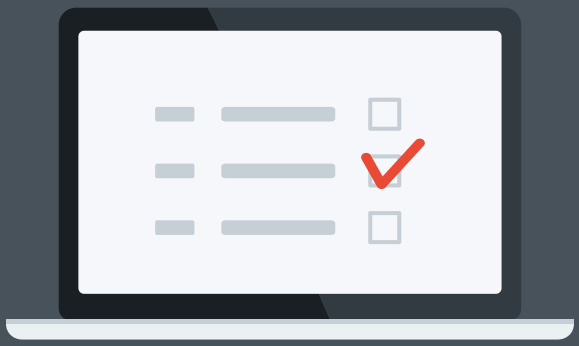
INFOSEC 2017 SURVEY REPORT

GDPR, the Cloud, and Government Spying



About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.

1. Executive Summary

1.1 Introduction

Infosecurity 2017 took place against a backdrop of change; so much change in fact, that some might call it chaos. The deadline for the GDPR moves ever-closer, but the British government is in a state of disarray at a time when negotiations to leave the EU are underway, all while it's trying to increase its surveillance capabilities as well.

Enterprises are feeling the brunt of these changes. While cloud, in all its various guises, continues to shape digital strategies, we were curious to find out how security professionals were adapting not just to cloud technologies, but also to the increased focus on privacy that the GDPR will bring within the overall context of a government that's eager to increase its powers.

The results are based on a survey of 918 attendees at InfoSecurity Europe 2017 and offer a glimpse into what security professionals feel the impact of changes related to the GDPR and cloud adoption could be for organizations.

1.2 Key Findings

- 50 percent of participants think the GDPR's 72 hour rule of breach notification could do more harm than good, and 42.6 percent reported that they were unsure if they could identify and report a data breach within 72 hours.
- 49 percent don't have or are unsure if they have data processing agreements with cloud providers, and 28 percent say that the level of cloud security expertise in their organization is either 'novice' or 'not very competent'.
- A significant section of respondents (37.5 percent) said that their organization would refuse to put a backdoor in their product if asked to do so by the government.
- The cybersecurity industry has a dim view of Theresa May's policies, which seek to undermine information security fundamentals like encryption and threat intelligence sharing.

1.3 Methodology

This report is based on experience of the author, a series of short discussions with security practitioners, and a survey of 918 participants at Infosecurity Europe 2017. It's important to keep in mind that the data analysis is based upon only this sample of participants. However, we do believe that this sample is representative of the larger information security industry and as such, provides us with useful insight upon which we can build our discussion.

Demographic data of survey respondents was not collected and respondents were not prompted for their answers nor was any clarification provided about the terms used or definitions.

This report was written by Javvad Malik, Security Advocate, AlienVault. Any questions about the methodology should be addressed to him at jmalik@alienvault.com.

2. Breach Notifications

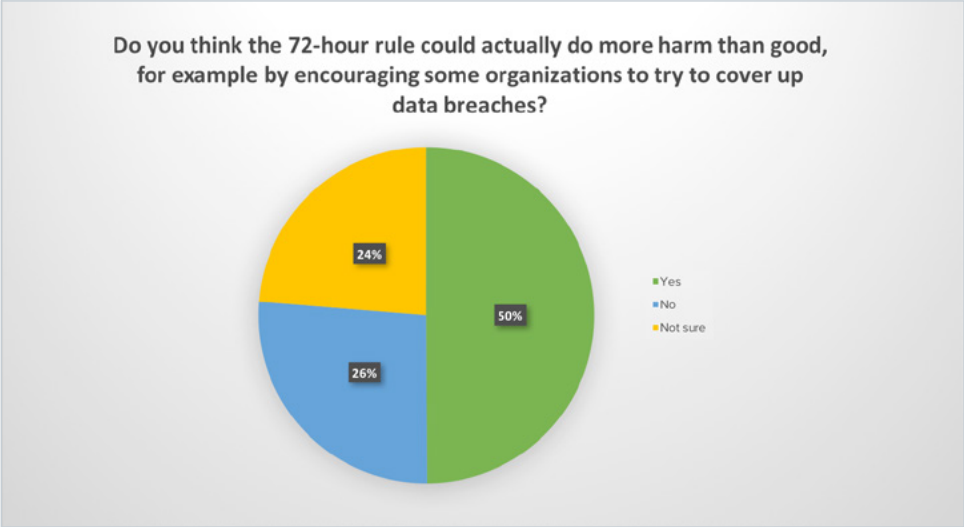
Article 31 of the GDPR states that "in the case of a personal data breach, data controllers shall without undue delay" and, where feasible and not later than 72 hours after having become aware of it, notify the supervisory authority of the personal data breach unless the breach is "unlikely to result in a risk for the rights and freedoms of individuals".

This section of the legislation has many companies apprehensive. Detecting a breach is by no means an easy feat for many enterprises. Given the difficulties often associated with collecting the information required to detect a breach, respond, ascertain the scope of damage, and identify potentially affected individuals, 72 hours starts to seem like it will be a very short window of time for most organizations.

Because of these factors, 42 percent of participants stated they are either not sure, or do not think they'd be able to identify and report a breach within 72 hours.

The balance that the GDPR is trying to achieve in requiring companies to report breaches is a tough one. While it's aim is to make organizations take more responsibility for the customer data they hold, the GDPR also recognizes the challenges enumerated above and allows companies to provide information in phases as it becomes available during the course of an investigation.

However, half of the survey participants felt that the 72 hour rule could actually do more harm than good because it could, for example, encourage some organizations to try and cover up data breaches so that they could avoid having to disclose and deal with the problem.



It's important to remember that the GDPR only mandates notification to the relevant supervisory authority in the case where there is a risk to the rights and freedoms of individuals. For example, the loss of personal data that could lead to discrimination, financial loss, or other economic or social disadvantage would fall under this scope.

The breach notification requirement will vary on a case by case basis. For example, if a breach results in systems being unavailable or log files being altered, but no customer details are stolen, then it would not need to be reported under the GDPR.

3. Where The Money Flows

As the GDPR looms ahead, it is interesting to take measure of how enterprises are preparing themselves.

26 percent of participants cited that the GDPR is encouraging their companies to increase spend in cybersecurity, while 17 percent have increased investments in legal departments.

45 percent of respondents indicated that their organizations are investing more in both legal and cybersecurity.

Given that GDPR isn't a cybersecurity-specific regulation, we did find the number of participants that stated an increase in cybersecurity funding was somewhat surprising. Perhaps this high percentage was due to fact that this survey was conducted at Infosecurity Europe, an event that attracts primarily information security professionals.

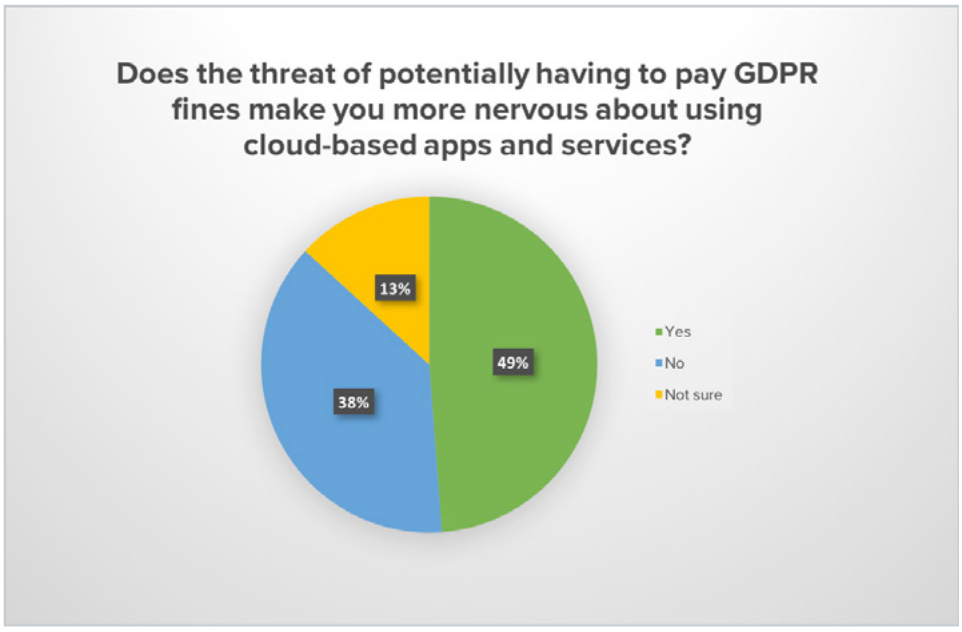
In practical terms, the GDPR covers much more than cybersecurity, or even legal aspects. Rather it is focused around privacy – and the need to protect it – which takes precedence over all aspects.

While the GDPR aims to make companies accountable through regulation, it would be naïve of them to treat the GDPR as merely a compliance exercise. The principles which form the basis of the GDPR focus on an enterprise's ability to uphold its obligations when it comes to cybersecurity and data protection. Ticking boxes will do little in that regard if companies do not adhere to the basic underlying principles or make an effort to put appropriate processes in place to ensure compliance.

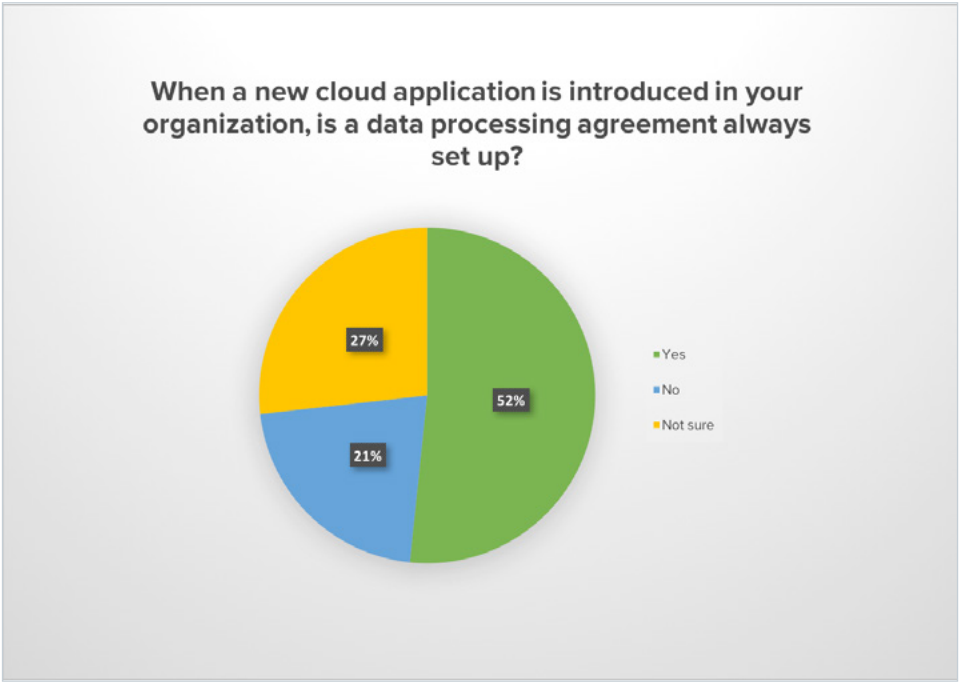
4. Cloud Regulations

The cloud throws another curveball into how companies consider the GDPR. Enterprises will need to be aware of where cloud providers store data, how that data is being stored, and how any processing takes place. In preparation, enterprises need to be aware that the regulation may necessitate new agreements with service providers, or even require companies to adopt completely new solutions altogether that conform to the standard of the legislation.

Although cloud services are widely used at organizations, nearly half the participants (49 percent) are afraid of falling afoul of GDPR because of their use of cloud-based applications. A further 13 percent indicated that they are unsure.



Reviewing their current cloud controls and processes would help companies be in a better position when the GDPR takes effect. However, when asked whether they always set up data processing agreements with cloud providers, 48 percent of participants indicated either that they do not, or are unsure of whether or not they do.

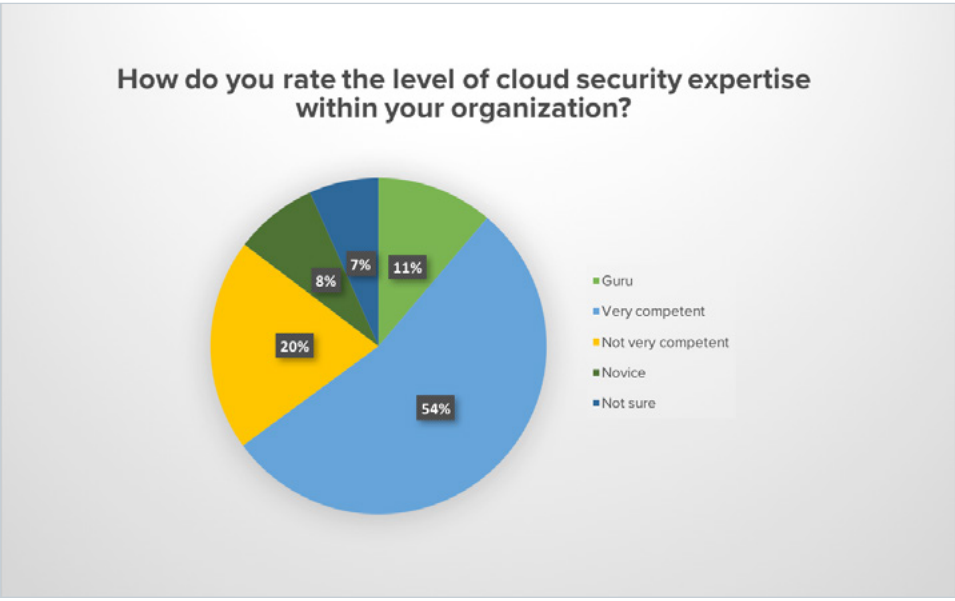


The GDPR may provide the impetus needed for companies to review existing agreements and set up new data processing agreements where needed. In addition, enterprises should keep an up-to-date inventory of all the personal information that they processe and store so they have a more comprehensive sense of what data might be at risk.

5. Cloud Expertise and Cutting Corners

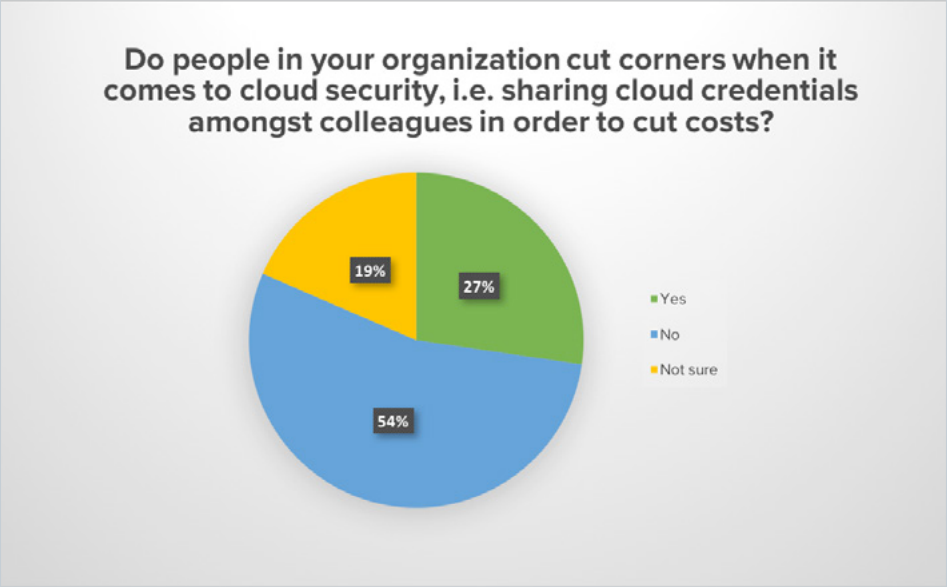
In order to function effectively in the cloud while remaining compliant, enterprises require a significant level of in-house cloud expertise to ensure that all processes and systems are appropriately configured and used.

However, when participants were asked to rate the level of cloud expertise within their organizations, only 18 percent ranked their organizations as possessing guru-level or very competent skills. Disturbingly, 20 percent reported that the expertise level at their organization was “not very competent” and a further 8 percent ranked it at “novice”.



This in itself suggests a worrisome state of affairs. While a cloud service provider will take care of many aspects of maintenance, uptime, and development, organizations themselves have responsibilities when it comes to the data they store, particularly related to classification, security, and access control, amongst others. Upholding these responsibilities will become even more critical when the GDPR takes effect.

Compounding the issue is that 27 percent of participants state that their companies cut corners when it comes to cloud security, allowing colleagues to share cloud credentials or licenses to cut costs.



While doing so may save a few dollars in the short-term, the lack of accountability that results from sharing cloud services can cost companies a lot more in the long run.

Cloud Security is a Shared Responsibility

Any company venturing into the cloud should have a fundamental understanding of the shared responsibility model and how it applies to cloud infrastructure-as-a-service (IaaS) security concerns.

Under the shared responsibility model, a cloud service provider (CSP) is generally responsible for ensuring the physical security of its data center, from building access to the securing of network and server hardware, and including oversight of the hypervisor hosting virtual machines. Cloud service users are responsible for securing their operating systems, applications and data running on cloud accounts.

It is important for organizations to bear this in mind when selecting cloud providers, particularly in light of the GDPR.

Organizations should also familiarize themselves with cloud security tools that are available to help them monitor their cloud infrastructure. For example, AWS CloudTrail can provide visibility into all cloud activities in the AWS environment. It can also feed data into cloud-based security management tools that can then provide cloud specific security capabilities such as centralized logging, firewalls, or file integrity monitoring.

6. Government Backdoors & Politics

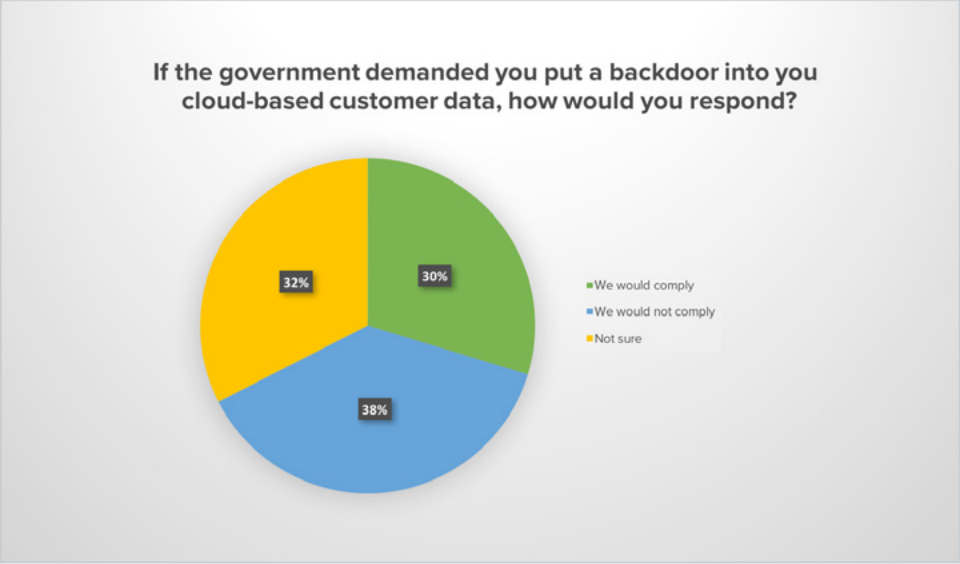
There is no doubt that cybersecurity has become critically important for both society and for governments today, because they now face an unprecedentedly high risk of external entities compromising or influencing core functionalities. For example, a number of recent elections around the world have generated copious discussion and speculation about whether electoral processes may have been hacked or compromised to sway the outcome.

Goverments can often feel like they have little control over their own security.

In fact, the rise of cybersecurity concerns combined with the widespread use of technology have given rise to a very contentious question: should governments be given backdoors to technology products? British PM Theresa May has long been waging a battle against encryption, stating that end-to-end encryption in apps like WhatsApp is "completely unacceptable" because it provides a safe-haven for terrorists.

The argument crops up repeatedly whenever there is a terrorist incident, and governments again begin to put pressure on technology companies to provide them with ongoing access to devices, either directly, or via backdoors installed just for them.

On the one hand, no-one wants to actively support terrorism, but including backdoors or weakening encryption introduces great risk to the overall security fabric of the internet, including banking, shopping and storage of medical records, amongst others – and thus could possibly cause harm that would outweigh the benefits of providing such access to government entities.



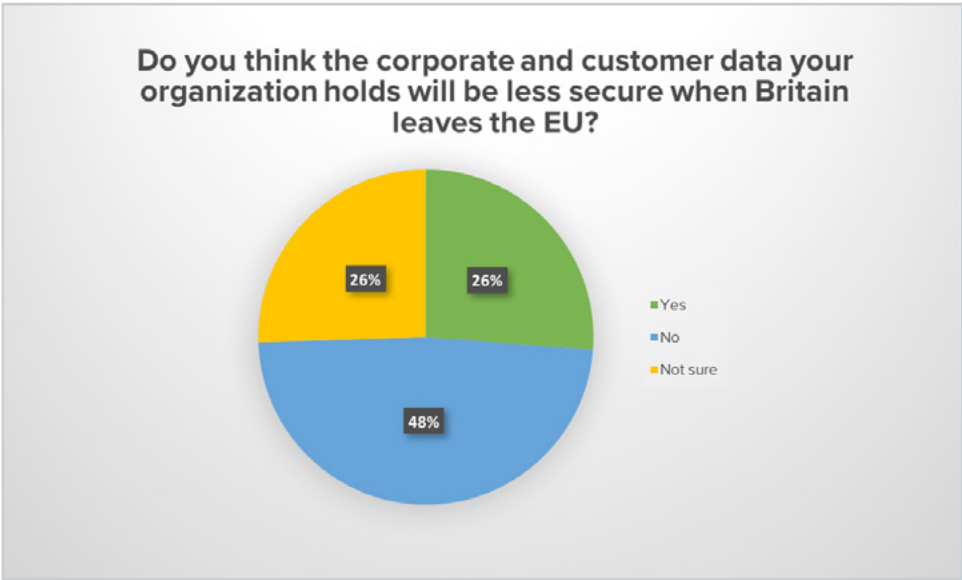
While 30 percent of respondents indicated that they would comply with a government request to add a backdoor to their products, a significant proportion of respondents (38 percent) said that their organization would refuse to do so.

Additionally, the opinions of the experts we interviewed weren't as divided as our survey data. In fact, every security expert we spoke with on camera agreed that backdoors were a bad idea.

This suggests that the government could find its proposals to limit encryption facing a long uphill battle.

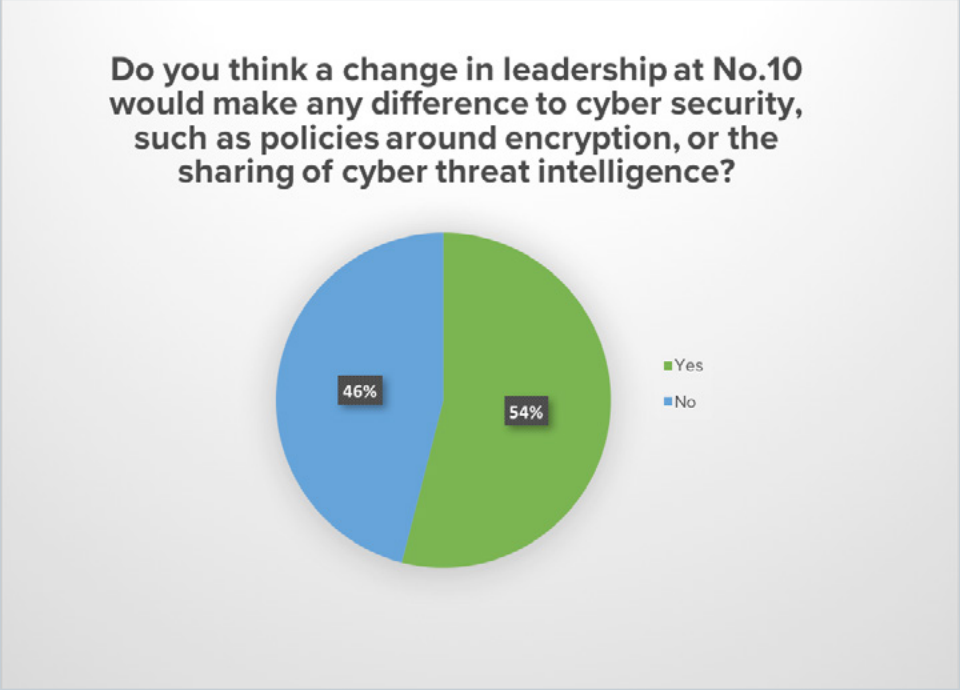
The cybersecurity industry has a somewhat dim view of Theresa May's technology policies, which oppose encryption and threat intelligence sharing, and 54 percent think that a change of leadership at No. 10 would make the country more cyber secure. The following comment sums up many of the attitudes expressed by survey respondents about May's leadership:

"Theresa May has literally no knowledge of the tech/security industry, and is using the standard rhetoric of sound bites about the industry in order to scare the electorate into voting"



The government has triggered article 50, beginning the official Brexit process of taking Britain out of the EU. Based on this, we asked participants how they felt Britain leaving the EU would impact security.

A quarter of participants felt that security of its corporate and customer data will suffer by Britain leaving the EU.



7. Conclusion

Why a collaborative approach is needed

A digital stalemate will remain as long as governments continue to beat the drum of wanting to weaken encryption or introduce backdoors.

However, this could potentially be resolved by turning the conversation around. Rather than governments trying to dictate methods that are either insecure or not feasible, they should list out their requirements for technology companies. Technology and security experts can then work through these requirements to make practical and feasible suggestions about how best to achieve the goals of maintaining privacy and security for customers while still being able to conform to legal requests for information.

Similarly, with the GDPR rapidly-approaching, enterprises need to ensure that appropriate attention is paid to all aspects—cybersecurity, legal, risk, compliance, and privacy—because all of these have a role to play. It is also important that organizations work with their cloud service providers as partners to ensure that the correct data processing agreements are in place.

While cloud offerings can benefit companies greatly, they do introduce different types of risks that need to be understood and effectively managed by enterprises. From a cybersecurity perspective, companies need to ensure that the right data processing agreements are in place, and also that they choose the right tools to allow them to manage their security.

Security complexities and challenges continue to grow, not just from a technological perspective, but from government, regulatory, and extended third party network requirements. With the GDPR set to take effect in May 2018, clear communication and effective collaboration that extends beyond corporate and geographical boundaries are more important today than ever so that organizations can continue to operate as secure and profitable businesses.

Appendix A

The Questions

Q1: If the government demanded that you put a backdoor into your cloud-based customer data, how would you respond?

a. We would comply
b. We would not comply
c. Not sure

Q2: Do you think the 72 hour rule could actually do more harm than good, for example by encouraging some organizations to try and cover up data breaches?

a. Yes
b. No
c. Not sure

Q3: Is GDPR encouraging your organization to invest more into its legal or cybersecurity department?

a. Legal
b. Cybersecurity
c. Both
d. Not sure

Q4: When a new cloud application is introduced in your organization, is a data processing agreement always set up?

a. Yes
b. No
c. Not sure

Q5: Does the threat of potentially having to pay GDPR fines make you more nervous about using cloud-based apps and services?

a. Yes
b. No
c. Not sure

Q6: How do you rate the level of cloud security expertise within your organization?

a. Guru
b. Very competent
c. Not very competent
d. Novice
e. Not sure

Q7: Do people in your organization cut corners when it comes to cloud security, i.e. sharing cloud credentials amongst colleagues in order to cut costs?

a. Yes
b. No
c. Not sure

Q8: If the government demanded you put a backdoor into your cloud-based customer data, how would you respond?

a. We would comply
b. We would not comply
c. Not sure

Q9: Do you think the corporate and customer data your organization holds will be less secure when Britain leaves the EU?

a. Yes
b. No
c. Not sure

Q10: Do you think a change in leadership at No.10 would make any difference to cybersecurity, such as policies around encryption, or the sharing of cyber threat intelligence?

a. Yes
b. No
c. Comment