RSA 2018 SURVEY REPORT

Re-thinking Security in the Privacy Era

Table of Contents

1. Executive Summary

1.1 Introduction

Privacy has always had a degree of overlap with security. However, in recent years the dependency each has on the other has increased in regards to protecting individual information, the use of social media, and the requirements to respond to breaches.

RSA Conference 2018 gave us an excellent opportunity to gather the opinions of InfoSec professionals. We were able to get a sizable number (759) and cross-section of respondents.

1.2 Key Survey Findings

- 61 percent believe that GDPR will protect EU citizens and 69 percent believe that similar laws would protect US citizens. 75 percent support additional regulations on social media platforms.
- While it was felt the board of directors, CEO, and CISO carry almost equal responsibility, in the event of a breach, the CISO would most likely be held responsible.
- 38 percent believe Mark Zuckerberg deserves to lose his job as CEO over the Cambridge Analytica scandal.
- Only 24 percent of companies believe they can expertly detect and respond to all types of security issues and catch most early enough in the lifecycle to mitigate impact.

1.3 Methodology

This report is based on experience of the author and a survey of 759 participants at RSA Conference 2018.

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

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

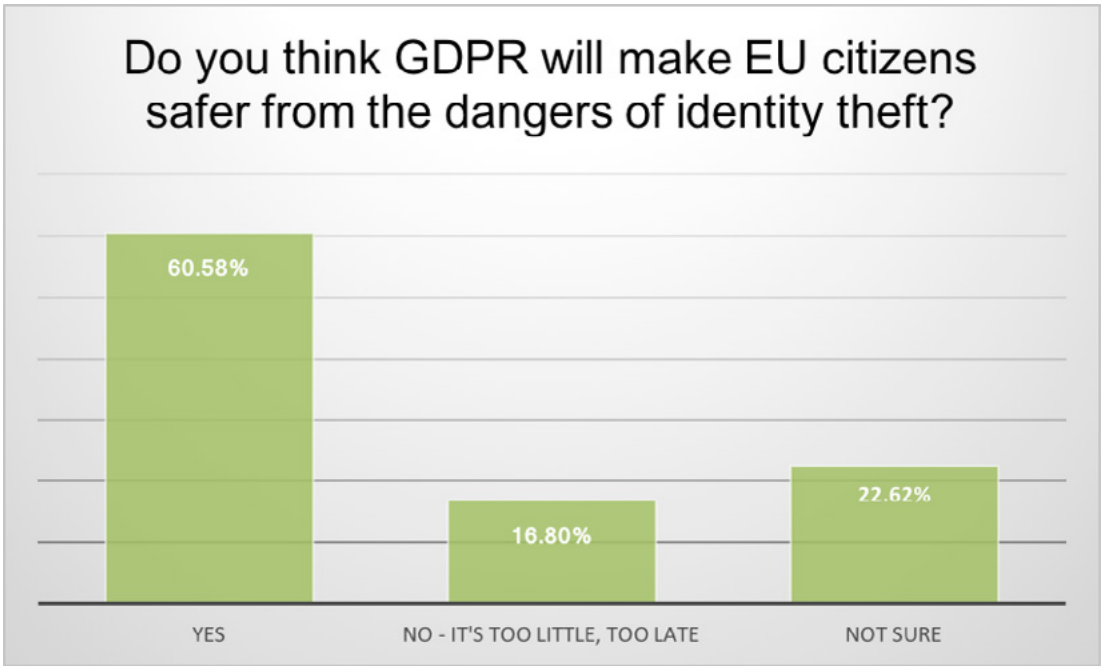
2. Privacy

2018 has been dominated by privacy news. This has been driven in part by new privacy regulations such as Europe's GDPR, or the updated Australian Privacy Act; and also by the Facebook and Cambridge Analytica revelations that have put a spotlight on how individuals' personal information can be used and abused in ways not previously considered.

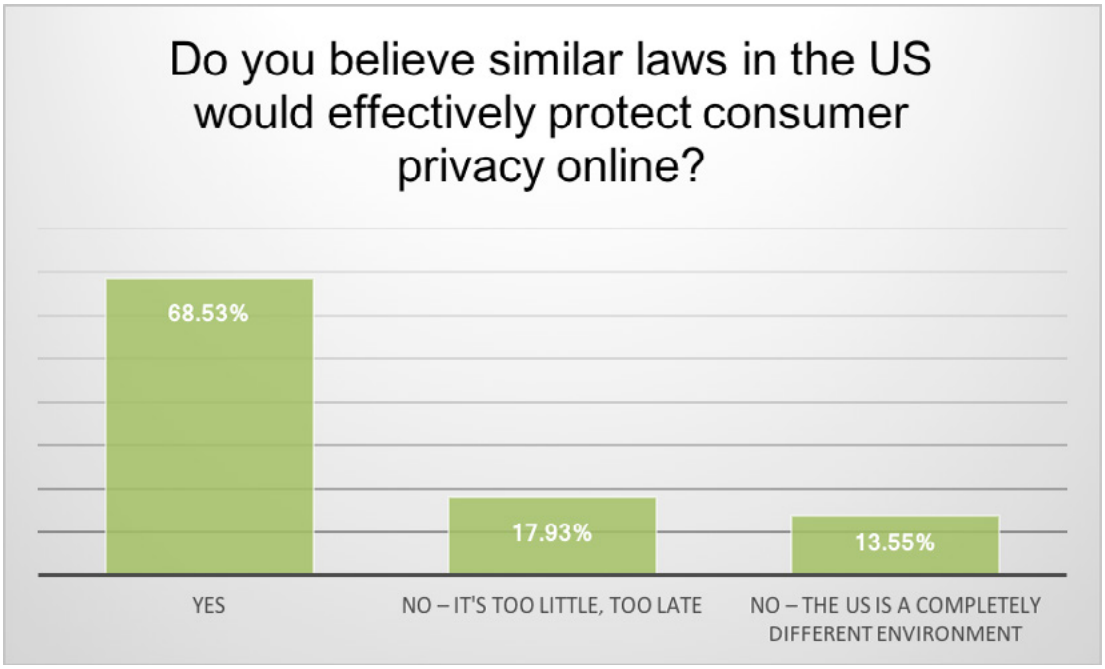
We saw companies trying to capitalize on privacy as a differentiator, such as Apple's CEO Tim Cook stating that the company has never profited through harvesting its customers' data.

But social media and products designed to capture vast amounts of individuals' data have been around for many years, so are regulations like GDPR a case of closing the barn door after the horse has bolted?

Our respondents at RSA didn't seem to think so, with an overwhelming 60 percent believing that GDPR will make EU citizens safer from the dangers of attacks such as identity theft.



That sentiment wasn't just restricted to the EU. Nearly 70 percent of participants also believed that similar laws in the US would be beneficial in protecting customer privacy online.



Practicality or Despair?

Usually regulation or compliance requirements are an unwanted part of business. The feeling is that they sometimes add an unnecessary burden on companies, or that they are largely ineffective.

So therefore, the broad support of regulations to protect individual privacy is a bit of an outlier.

Maybe there's a sense of despair that, left to their own devices, organizations would only accumulate more and more data that is not only poorly secured, but used to build comprehensive user models.

It's often been quoted, "If you don't see the product, you are the product." The reality for most users is that they haven't had a good idea as to what 'being the product' means until now.

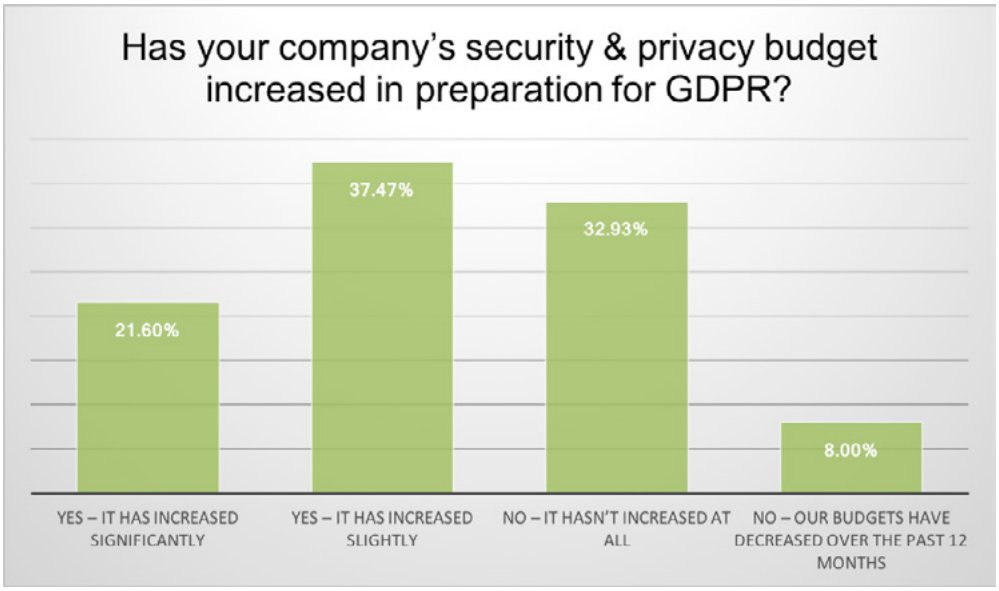
Given the environment that has been created, telling users not to share their information online is not sufficient. Big data models pull in information from a variety of different sources, and data is collected and sold through many channels – which is why the onus should be put on companies to ensure information collected, processed and stored is done so in a responsible manner.

GDPR Impacting Budgets

Meeting any new regulatory or compliance standard does require effort on the part of companies. Some, more so than others.

Of the participants, 22 percent stated their company's security and privacy budget increased significantly to meet the needs of GDPR.

While 33 percent stated their company's budget didn't increase at all because of GDPR, 8 percent said it actually decreased over the past 12 months.



Too Much Regulation?

The broader question is whether too much regulation has the danger of raising the entry barrier for online businesses.

Online businesses that sell products to users now not only have to ensure their sites are adequately protected from all common forms of web attacks, but they have to demonstrate compliance to regulators in order to meet the requirements laid out by PCI DSS or GDPR. Additional requirements may arise from partners wanting to conduct third- party assurance.

A combination of these factors will likely drive businesses increasingly down the route of cloud adoption. While cloud won't necessarily tick all the security boxes - after all, it is still the company as the data owner's responsibility to secure its data, not the cloud provider - it does remove a large regulatory burden in many areas for companies looking to grow.

3. Responsibility

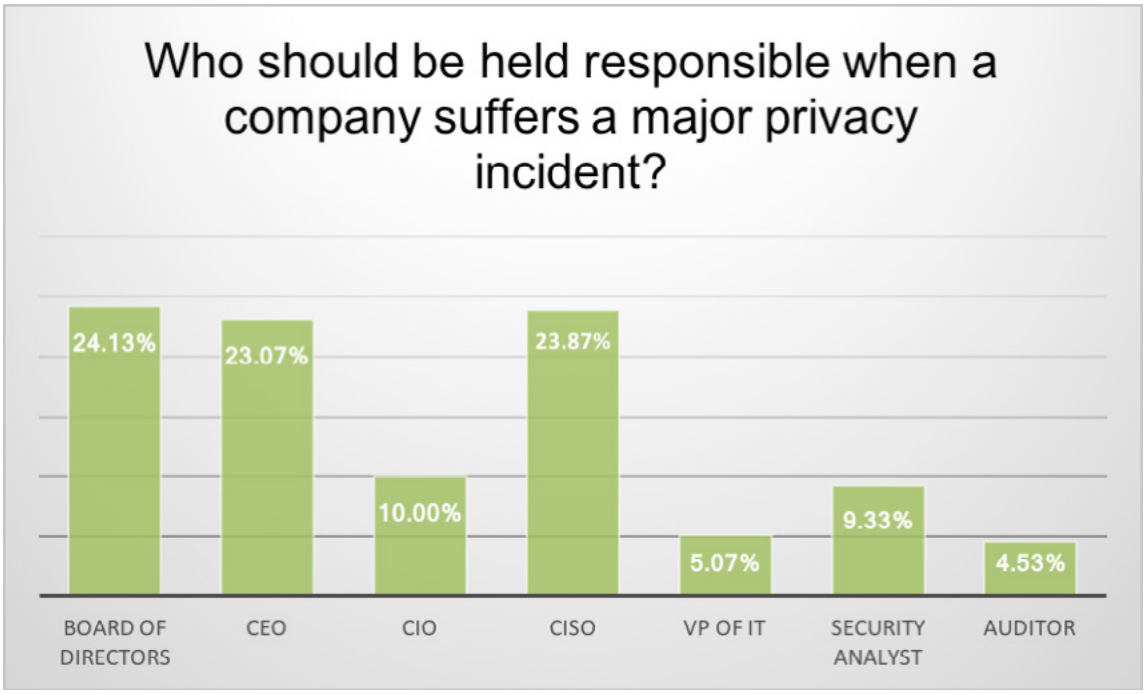
Many companies have dedicated security teams, but security isn't just their responsibility. It extends into other departments as well as up the chain. After all, the tone is set from the top.

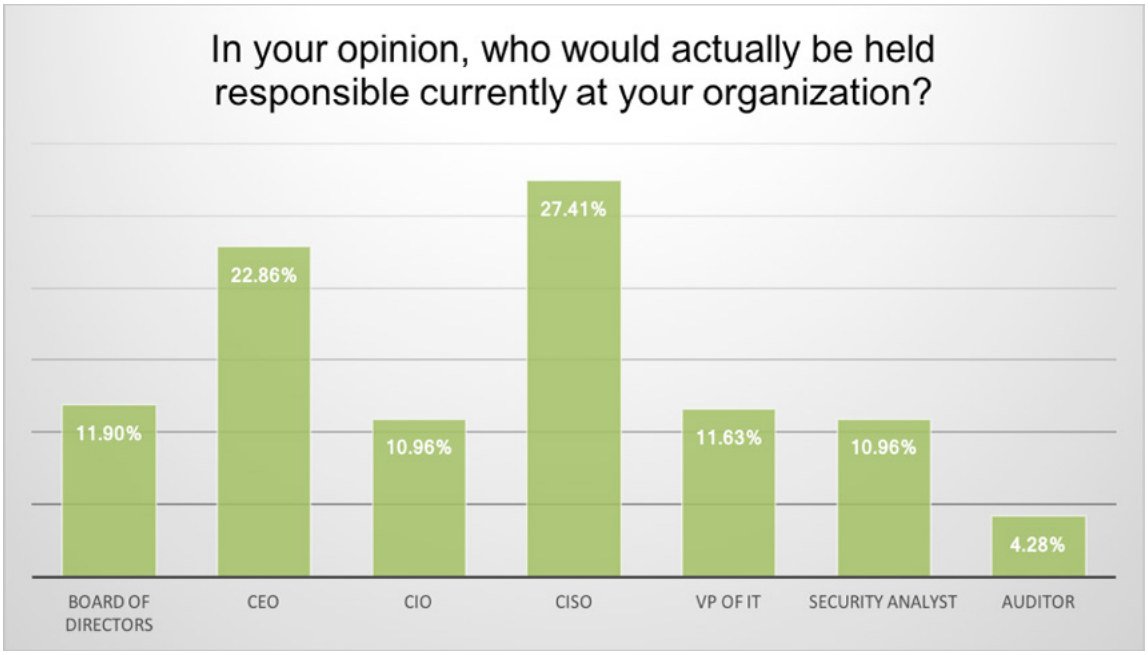
We asked participants who, in their opinion, should be held responsible when the company suffers a major privacy incident versus who will likely be held responsible.

In terms of who should be held liable, opinion was almost evenly split between the board of directors, CEO, and the CISO.

However, most felt that in reality, in the wake of an incident the CISO will be the one left holding the can, followed closely by the CEO.

The biggest difference was with the board of directors. 24 percent believed the board should carry some of the responsibility of a privacy breach, but only half of those, 12 percent, believed the board would actually be held accountable.





However, a security or privacy incident reflects poorly upon many areas of a business and could have far-reaching consequences. The company formerly known as Yahoo was recently fined $35 million for failing to disclose a data breach which occurred some four years earlier in 2014.

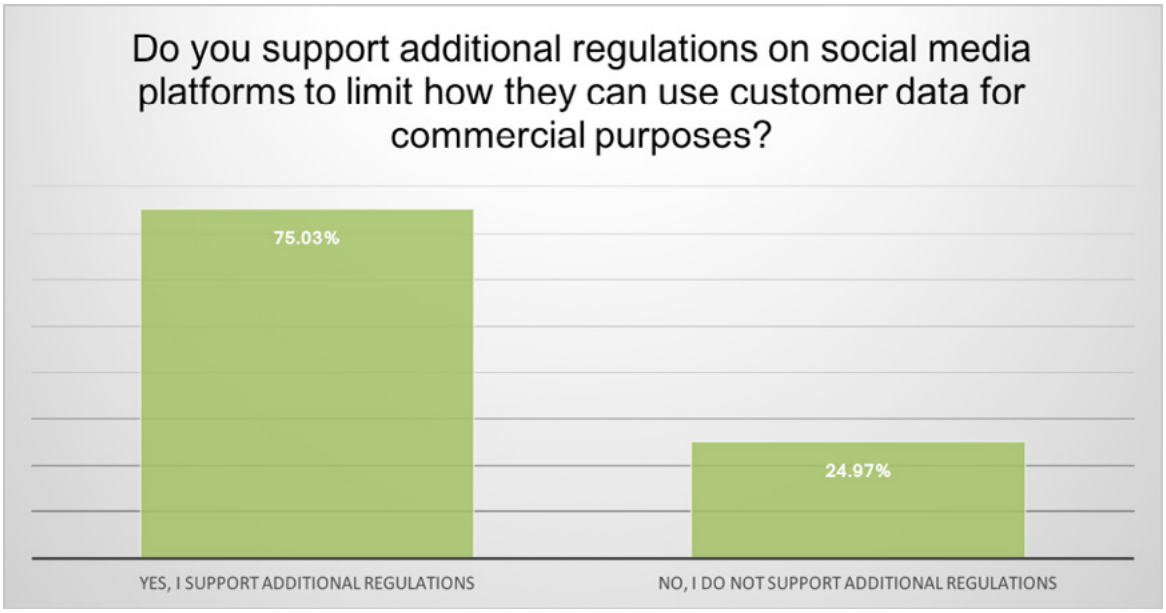
Therefore, it's not surprising to see 57 percent of participants stated their senior management were very concerned about security, with 31 percent stating they were somewhat concerned.

Only 4 percent stated their company's senior management were not concerned at all about security.

4. Facebook

Facebook has made headline after headline over the course of 2018 for all the wrong reasons. Cambridge Analytica, misleading political advertisements, and an overall cavalier attitude towards customer privacy have the company in the crosshairs of many privacy groups as well as users.

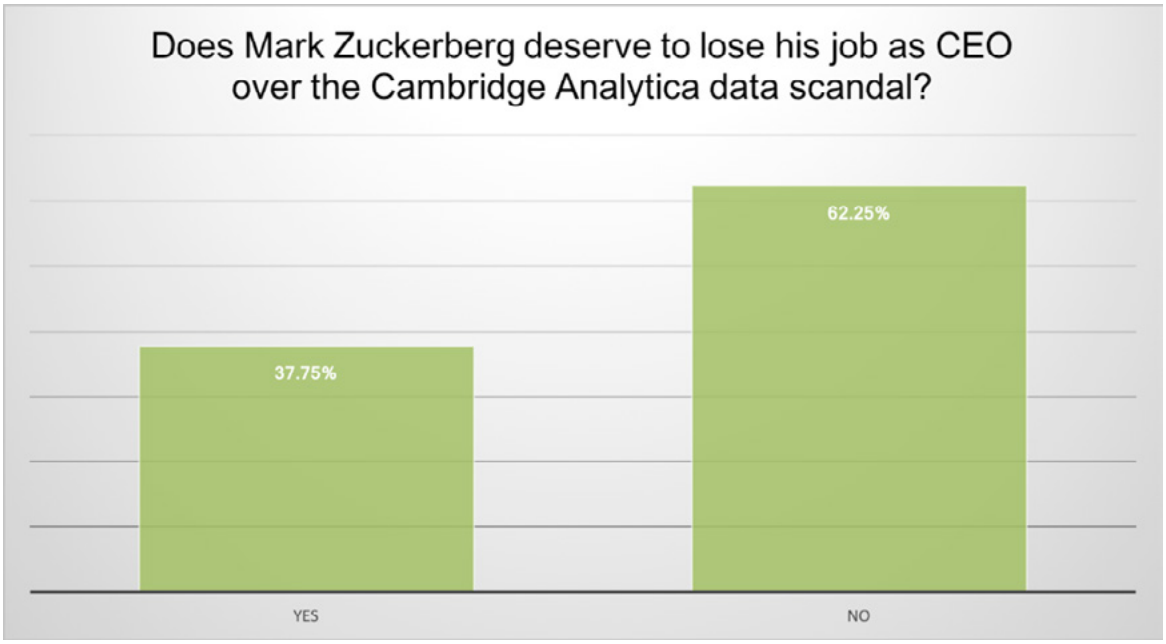
75 percent of participants support additional regulations on social media platforms to limit how they can use customer data for commercial purposes.



This is an interesting perspective and ties back to the overall desire for more privacy protection through regulation – hinting at the lack of faith users have in social media companies being able or willing to regulate themselves.

Interestingly, only 38 percent of respondents believed that Mark Zuckerberg deserved to lose his job as CEO over the Cambridge Analytica scandal.

In some ways, it's hard to imagine who would be a good replacement for Zuckerberg if he were to step down as CEO. Facebook has grown in reach and influence beyond any social network that came before it, so it's not like there is a shortlist of CEOs qualified to steer the company in a clear direction.



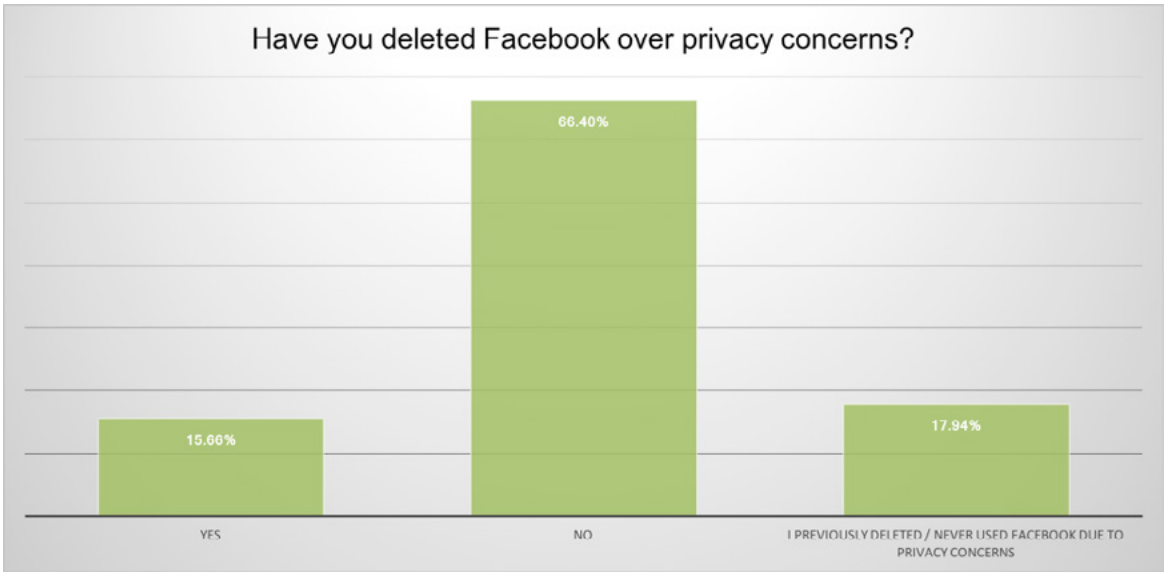
Facebook Theory vs Reality

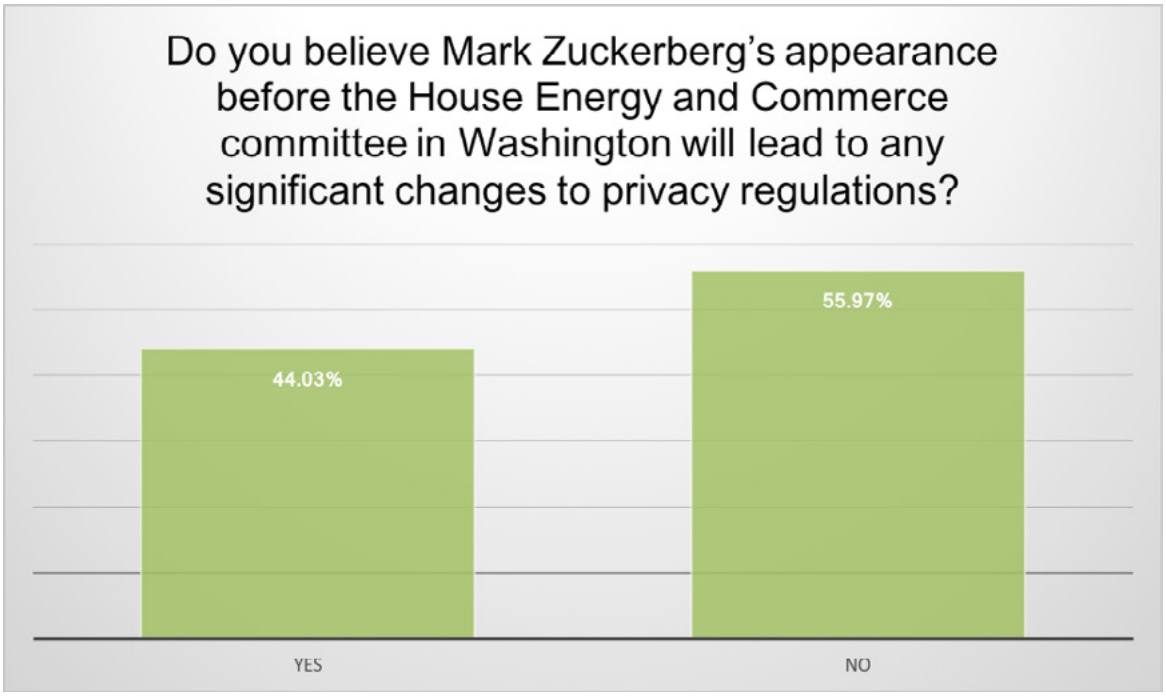
While there has been much outrage over the Facebook/Cambridge Analytica scandal, only 16 percent of participants stated they deleted Facebook over privacy concerns. Another 18 percent stated they had already deleted Facebook or never used it to begin with because of privacy concerns.

The vast majority, at 66 percent, stated they hadn't deleted Facebook over privacy concerns.

It sheds light on two interesting perspectives. There is a real-world dependency on Facebook for many that allows them to stay in touch with family and friends around the world. So, even in the light of privacy issues, leaving the platform may not be a viable solution when it is interlinked with others.

The second viewpoint is a lot broader in that it isn't necessarily a Facebook issue but a general social media and technology issue. Data is the most valuable of resources; it is acquired and used by a whole plethora of companies. Even if Facebook ceased to exist tomorrow, the privacy challenge will remain. A challenge that no-one seems to know the answer to – reflected by the fact that 56 percent of participants were doubtful that Zuckerberg's appearance before the committee in Washington would lead to any significant changes to privacy regulations in the US.





5. Threat Detection

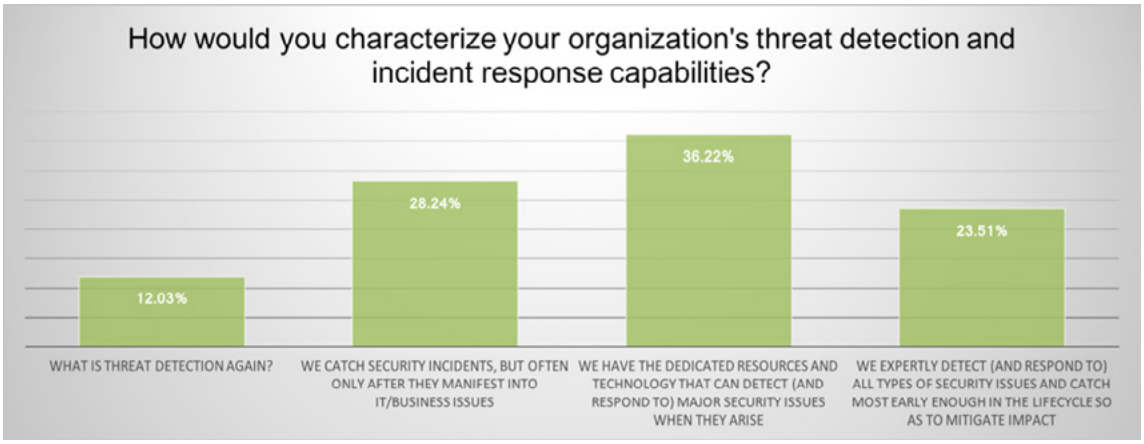
Threat detection and response is an important requirement for GDPR. Most participants were confident in their threat detection capabilities, with 65 percent stating they would be able to report a privacy breach within 72 hours of becoming aware.

Of course, the key phrase here is 'being aware.' The real challenge for many companies is detecting threats when they occur.

To this point, 28 percent stated their ability to detect a threat was often only after it had manifested into a business issue.

A further 36 percent were confident they had the tools and capability to detect and respond to major security issues when they arise.

Only 24 percent classified themselves as being able to expertly detect and respond to all types of security issues.



The Haves and Have-nots

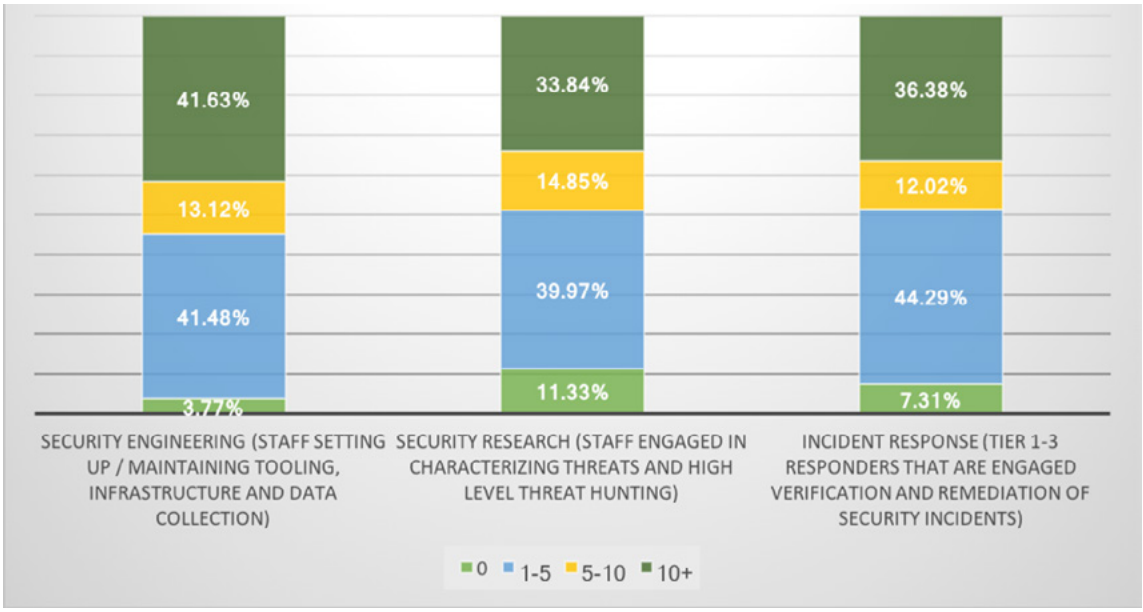
We asked participants on the size of their security teams across engineering, research and incident response.

It became clear that there are two broad camps – companies that have between one and five employees in each discipline, and those that have over 10.

This highlights an almost equal split between companies and their approaches to security. Having large teams of over 10 people enables companies to be well-equipped to install and manage a multitude of security technologies, spend time assuring the technologies work as desired, and document processes and procedures.

However, over half the market does not have the luxury of 10-person teams, so their resources are spread thin, with individuals likely having to wear multiple hats to keep technology and security running smoothly.

In such environments, having a selection of disparate security tools is not feasible, which is why it's important for security to be designed in a way that it can be easily adopted and utilized by enterprises with small teams. As such, having multiple capabilities pre-integrated and performing a wide range of security and compliance activities is easier to manage for these companies.



Conclusions

Privacy has traditionally been viewed as a distant cousin of security, but the two disciplines have formed an ever-increasing dependency on each other in recent times. While there is a business incentive for companies to invest in security, similar incentives don't necessarily exist for companies to protect their customers' privacy. In fact, a lack of customer privacy can help the bottom line.

Therefore, it doesn't come as a huge surprise that many support regulation as a means to force the hand of companies to take the privacy of their customers and users more seriously.

Cyber security has come a long way from the days of merely being an IT function. It is very much embedded as a fundamental business requirement. However, the scope and impact of its responsibility haven't evolved at the same pace – or at least haven't appeared to do so. Which is why it appears that the CISO will bear the brunt of the blame in the event of an incident.

With threats ever-increasing, companies are investing more in threat detection and response capabilities. Some of these investments are driven through regulatory requirements, and others because of the progressing security maturity.

But there is a gap between companies that can invest significant resources into security and those that can't. It is therefore imperative that smaller teams be catered to accordingly through increased staff awareness, better training, or more comprehensive and easy-to-deploy (and use) security technologies. If not, we will only see an increase in successful attacks and breaches against the companies that can afford it the least.

Appendix A

The Questions

1. Do you think GDPR will make EU citizens safer from the dangers of identity theft?

   a. Yes
   b. No - it's too little, too late
   c. Not sure

2. Do you believe similar laws in the US would effectively protect consumer privacy online?

   a. Yes
   b. No – it's too little, too late
   c. No – The US is a completely different environment

3. Has your company's security & privacy budget increased in preparation for GDPR?

   a. Yes – It has increased significantly
   b. Yes – It has increased slightly
   c. No – It hasn't increased at all
   d. No – our budgets have decreased over the past 12 months

4. Under GDPR, organizations are required to report a privacy breach within 72 hours of becoming aware. Regardless of whether GDPR applies to you, do you believe your organization currently has the procedures in place to meet this requirement effectively?

   a. Yes
   b. No
   c. Unauthorized file sharing

5. Who should be held responsible when a company suffers a major privacy incident?

   a. Board of Directors
   b. CEO
   c. CIO
   d. CISO
   e. VP of IT
   f. Security Analyst
   g. Auditor

6. In your opinion, who would actually be held responsible currently at your organization?

   a. Board of Directors
   b. CEO
   c. CIO
   d. CISO
   e. VP of IT
   f. Security Analyst
   g. Auditor

7. How concerned is your company's senior management about security?

   a. Very concerned
   b. Somewhat concerned
   c. Not very concerned
   d. Not concerned at all

Appendix A

The Questions

8. Do you support additional regulations on social media platforms to limit how they can use customer data for commercial purposes?

    a. Yes, I support additional regulations
    b. No, I do not support additional regulations

9. Does Mark Zuckerberg deserve to lose his job as CEO over the Cambridge Analytica data scandal?

    a. Yes
    b. No

10. Have you deleted Facebook over privacy concerns?

    a. Yes
    b. No
    c. I previously deleted / never used Facebook due to privacy concerns

11. Do you believe Mark Zuckerberg's appearance before the House Energy and Commerce committee in Washington will lead to any significant changes to privacy regulations?

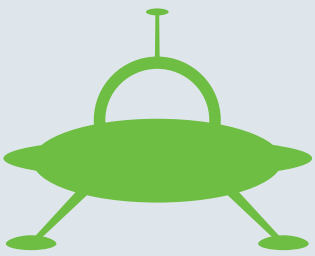
    a. Yes
    b. No

12. How would you characterize your organization's threat detection and incident response capabilities?

    a. What is Threat Detection again?
    b. We catch security incidents, but often only after they manifest into IT/Business issues
    c. We have the dedicated resources and technology that can detect (and respond to) major security issues when they arise
    d. We expertly detect (and respond to) all types of security issues and catch most early enough in the lifecycle so as to mitigate impact

13. How many of your full-time staff or part-time staff equivalent are engaged in the following activities: {ranges, 0, 1-5, 5-10, 10+}

    a. Security Engineering (Staff setting up / maintaining tooling, infrastructure and data collection)
    b. Security Research (Staff engaged in characterizing threats and high level threat hunting)
    c. Incident Response (Tier 1-3 responders that are engaged verification and remediation of security incidents)



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.