proofpoint.

REPORT

THE GREAT DISCONNECT

PERCEPTION AND REALITY OF GDPR READINESS IN THE UK, FRANCE AND GERMANY

proofpoint.com

On 25 May 2018, the General Data Protection Regulation (GDPR) will come into effect globally. The new regulation is designed to strengthen and unify data protection for everyone within the European Union (EU). They also regulate how personal data is exported outside the EU. With six months to go until GDPR comes into force, Proofpoint commissioned a benchmarking survey to answer three key questions:

- How are organisations are preparing for GDPR compliance?
- How advanced are their implementation plans?
- How confident are they of achieving their goals by May 2018?

The survey, conducted by Censuswide between 22–29 September 2017, polled 1,500 IT decision-makers from companies with 200 or more employees in the UK, France and Germany. The firm collected data from 500 participants per country across a range of industries.

This report highlights the results of the survey. We explore how businesses are preparing for the impending regulation across the UK, France and Germany. And we analyse differences between industry sectors to see which are most at risk of non-compliance.

GDPR OVERVIEW

GDPR replaces the 22-year-old EU Data Protection Directive. At its core, the GDPR aims to put EU residents in control of their personal data. It regulates how their data is collected, processed, stored, deleted, transferred and used.

No matter where it is based, any company that does business in Europe or handles the personal data of EU residents must comply with the new rules.

Developing a plan to comply with the new rules is critical for all organisations. Failure to do so could lead to unprecedented fines of up to 4% of annual global revenue or €20,000,000, whichever is higher. This amount is far higher than any penalties data protection authorities (DPAs) within EU countries can issue today.

The timer has started—organisations have just six months left to prepare for the impending deadline. But many businesses are arguably confused about what successful compliance means.

Many questions remain. What changes will have to be made to internal processes to comply? What technologies should companies leverage to ensure that the personal data of EU residents are protected? How can IT and security professionals embed 'privacy by design' into their development lifecycles?

One thing is clear, though: organisations must act now to deploy people, process and technology controls that protect EU personal data. Privacy is increasingly seen as a business enabler. GDPR offers businesses a great opportunity to benefit from its implementation.

"Tackling this new set of rules requires important changes for all organizations that handle customer data, but it comes with a golden opportunity for security, risk, and privacy professionals. In times when privacy grabs the board's attention and organizations are growing their privacy budgets, security, risk, and privacy folks have the chance to elevate the privacy discussion from a mere compliance need to a business strategy for growth."

The EU General Data Protection Regulation (GDPR) Is Here, April 2016 Forrester Blog Post, Enza Iannopollo.

RESEARCH FINDINGS

Here are our key findings from the research:

- **Data breaches are the new normal**
- **Organisations may be less ready than they think**
- **GDPR compliance is not on the executive agenda**
- **Many organisations are bracing for the consequences of non-compliance**

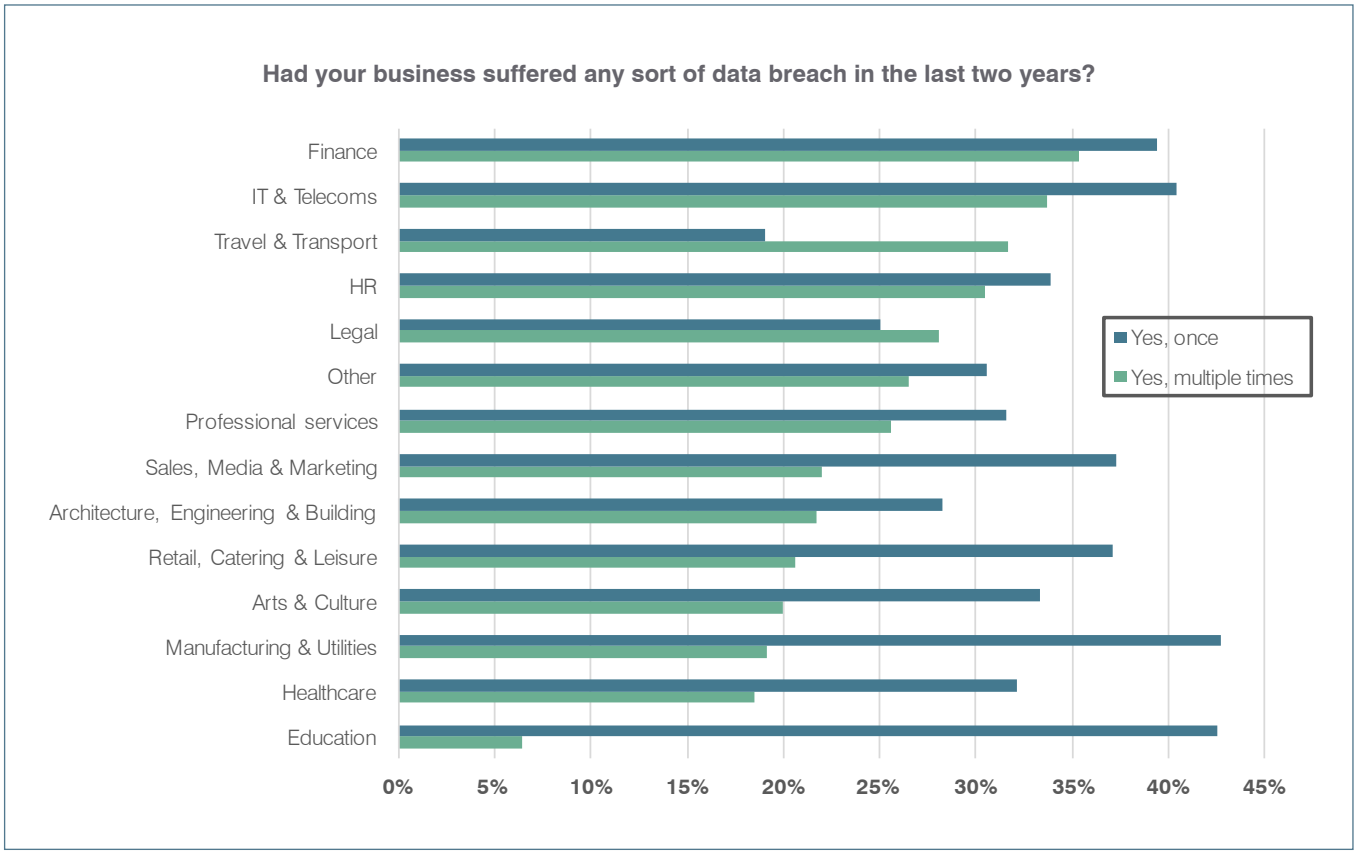
DATA BREACHES ARE THE NEW NORMAL

Cyber attacks have long been a fact of life for security professionals. In the wake of blockbuster attacks and massive data breaches, these risks have been thrust into the mainstream.

Two recent high-profile attacks made the topic almost impossible to ignore. The Equifax breach exposed the private data of more than 145 million Americans and the WannaCry ransomware attack infected more than 200,000 machines across 150 countries.

Data breaches are both more common and more widely reported today than ever before. Organisations might have once assumed that security breaches affected the unfortunate few. Today, most realise that attacks aren't a question of "if", but of "when".

In our survey, 64% of respondents said they suffered a data breach at least once in the last two years. All reported breaches included personal data. At the current rate of breaches, nearly two-thirds of businesses in Europe could be liable and subject to fines. (Under GDPR rules, organisations must protect the confidentiality and integrity of personal data. They must also disclose any beaches within 72 hours.)



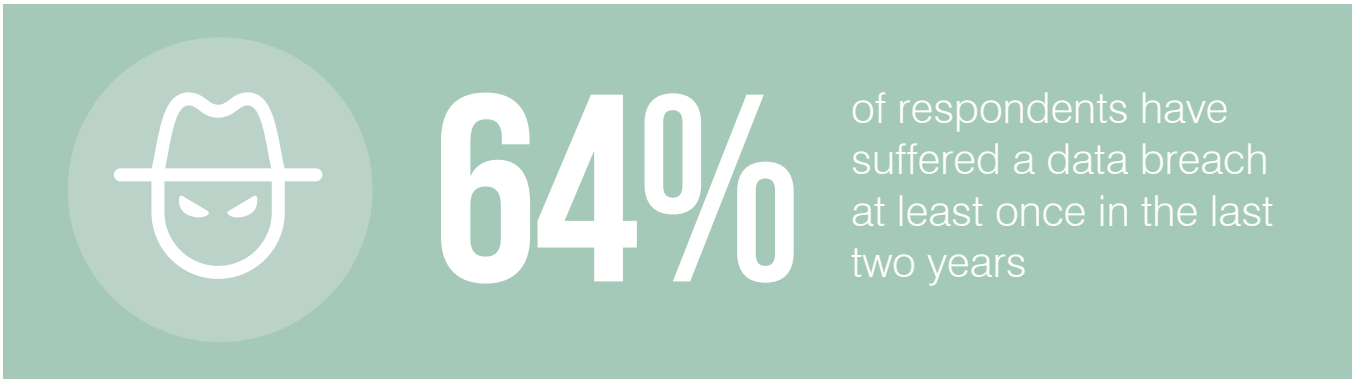
Of the three countries surveyed, companies in France have suffered the highest percentage of multiple breaches in the last two years at 29%. French companies also appear to have a heightened awareness of their risk of being breached. About 78% of survey respondents in France said their businesses are likely to suffer a data breach in the next 12 months. Just 54% of respondents in the UK and 46% of respondents in Germany said the same.

When it comes to targeting industries, cyber criminals share at least one thing in common with their counterparts in the physical world: finance attracts the most attention.

Some 35% of financial institutions report that they had suffered a data breach multiple times in the last two years. That's much higher than the 19% rate for healthcare, manufacturing and utilities.

Financial organisations have processes and technologies to detect and respond to any breaches. Much of that is due to industry regulations. Sarbanes–Oxley (SOX) and the Financial Industry Regulatory Authority (FINRA) are two examples.

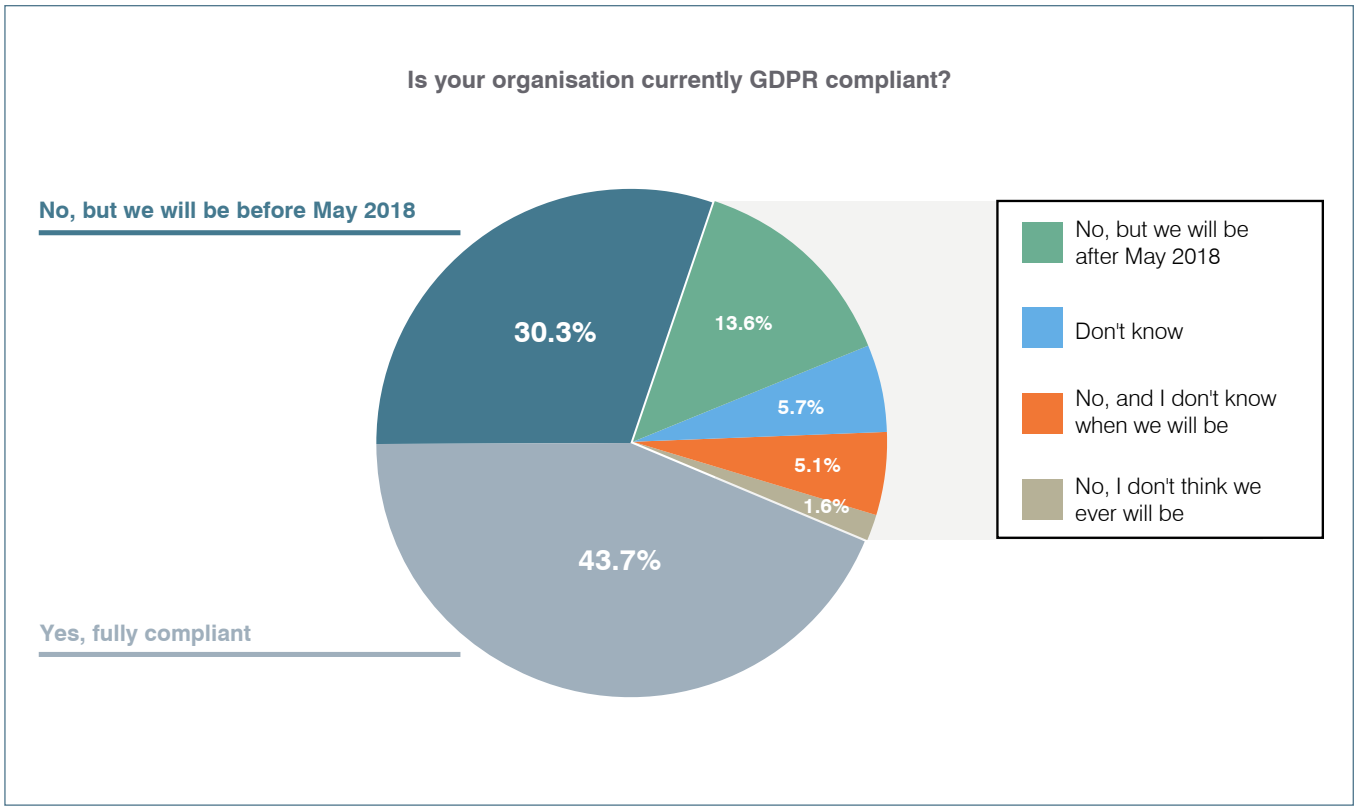
Other industries, however, have been slower to adapt.



GDPR READINESS: PERCEPTION IS NOT REALITY

Nearly two-thirds of survey respondents admit they have suffered a breach over the course of the last two years. Despite this reality, businesses are bullish about their ability to comply with the GDPR by the May 2018 deadline.

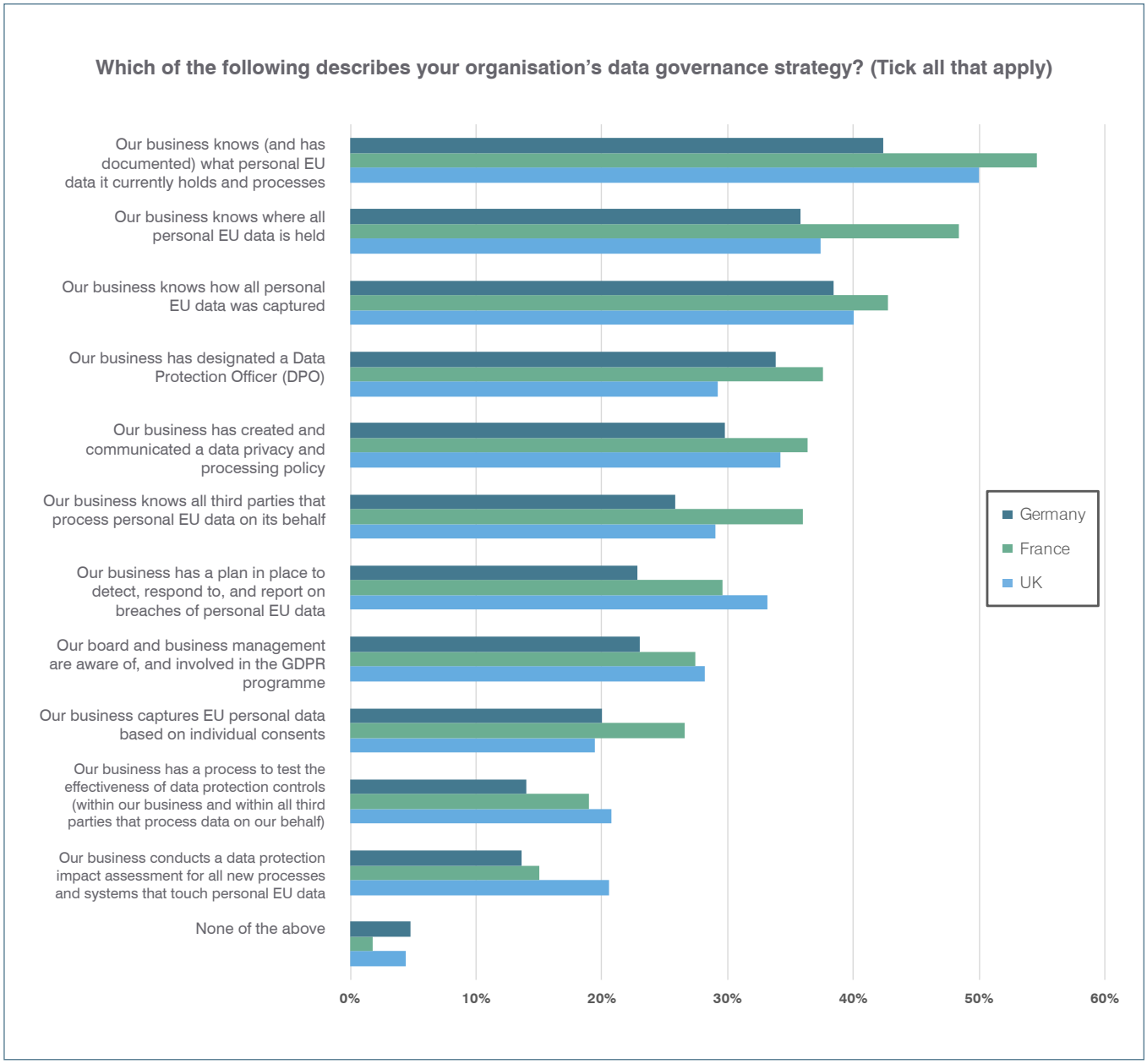
According to the survey, 44% of businesses in the UK, France and Germany believe that they are already fully compliant with the GDPR. And 30% believe that they will be compliant before May 2018.



At best, this optimism could be described as naïve.

Only 49% of businesses know and have documented the personal EU data that they process. And despite having two years to prepare (the GDPR was adopted in April 2016), only 40% of those surveyed have completed a GDPR readiness assessment.

Just 28% of businesses have a plan in place to detect, respond to, and report on breaches of personal EU data. The situation may not get much better anytime soon. Research firm Gartner forecasts that by the end of 2018, more than half of companies affected by the GDPR will not be in full compliance.



Comparing industries, our survey shows healthcare is behind when it comes to data governance maturity. This finding may not be surprising, but it is worrying. Data collected by public and private healthcare firms is hugely valuable for cyber criminals—medical data is worth 10 times more than a credit card number on the black market —and incredibly sensitive.

Many healthcare organisations are using cloud technology to serve patients in innovative ways. They're collecting and storing more records digitally but still use paper records. They often use old, IT technologies, which can be vulnerable to new cyber attacks. And they deal with especially sensitive data. Disparate data stores mean that some don't even know where all of their personal data resides.

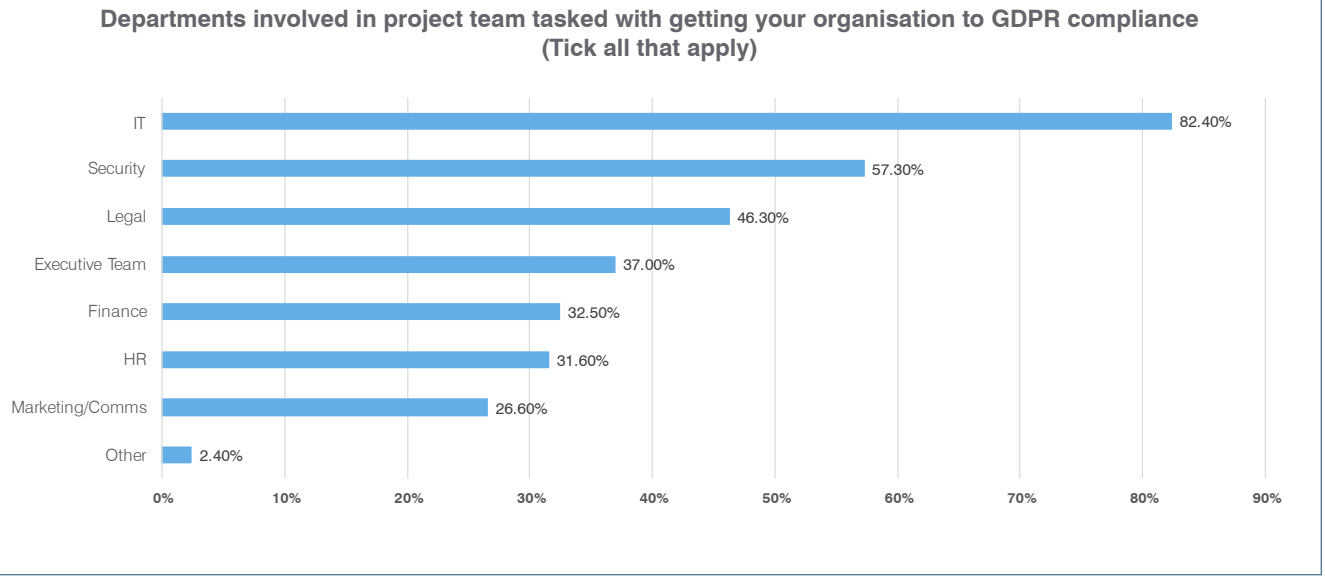
At this stage, the GDPR is all about how organisations choose to interpret the various principles within the regulation. This ambiguity—and organisations' misplaced confidence in their GDPR readiness—is leading to inertia. Companies are not taking the steps they need to take to comply.

GDPR COMPLIANCE NOT ON THE EXECUTIVE AGENDA

Under the GDPR, responsibility lies with multiple internal and external stakeholders. Many organisations are unclear about where ownership should fall. That ambiguity is hindering the processes that need to be put in place to be compliant.

A majority of organisations (74%) have a cross-departmental team in place to drive the business to GDPR compliance. But only 26% of IT decision makers say their board of directors and executive business management are aware of and involved in their GDPR programme.

Without executive buy-in and involvement, organisations will struggle to implement the changes required to meet compliance.



For most businesses, security and IT are responsible for ensuring GDPR compliance. Our survey found that 82% of organisations' IT teams are involved in getting the business to compliance vs. just 27% of marketing teams. CIOs are leading the charge, but GDPR is more than an IT or security initiative—it affects every department.

The driving role of IT in compliance is reflected in increased investments. Some 66% of IT decision makers say that their budgets have increased in the run-up to May 2018. At the same time, 57% say that compliance and regulation are driving their security programmes today. These totals suggest GDPR presents a golden opportunity for security and IT teams to grab the attention of their boards.

GDPR has highlighted the need for effective cybersecurity. That means IT and security teams can secure the budgets they need to deploy innovative cybersecurity strategies and roadmaps. Driven by compliance, cybersecurity has become a top priority in the ever-growing list of business imperatives.

26%

of IT decision makers stated that their board and business management are aware of and involved in their GDPR programme

66%

of IT decision makers say that their budgets have increased in the run up to May 2018

57%

of IT decision makers say that compliance and regulation are driving their security programmes today

MANY ORGANISATIONS ARE RESIGNING THEMSELVES TO NON-COMPLIANCE

At this stage, GDPR is all about interpretation. That may be why many organisations are choosing to mitigate their risk exposure rather than strive for full compliance.

Businesses know they need advanced information and cybersecurity controls. They also know that they're expected to comply with the GDPR. But due to the perceived complexity, some are instead preparing to manage the fallout of non-compliance.

39%

of businesses believe they are financially prepared to cover the fines once GDPR is in effect

24%

of respondents state that they have purchased cyber insurance in case of a breach

Some organisations believe they understand the financial risks associated with non-GDPR compliance after May 2018. In our survey, 39% of businesses say they are financially prepared to cover the fines once GDPR is in effect.

Some organisations have opted to transfer risk. Nearly a quarter (24%) of respondents say that they have purchased cyber insurance in case of a breach.

Cyber insurance can help cushion the cost of a breach. That includes secondary costs such as the expenses of containing, communicating, investigating and remediating it. But many insurance policies will not cover fines from non-compliance to the GDPR principles. That's why you need multiple layers of defense. These layers should include technical and organisational controls that protect the integrity and confidentiality of EU personal data.

HOW YOU CAN PREPARE FOR GDPR: PROTECTING KEY ASSETS

Before they can move towards full compliance, organisations must first fully understand the requirements. All the GDPR rules and requirements fall under one of seven key principles.

Principle 6, Integrity and Confidentiality, states that personal data should be rendered anonymous where possible. This anonymisation ensures that EU residents can no longer be identified by the data. For data that cannot be made anonymous, GDPR requires technical and organisational controls to safeguard the processing of any personal data.

Responsibility to protect data will no longer fall only upon the businesses that collect data from EU residents. Under GDPR, third-party data processors are responsible for keeping personal data entrusted to them private. Our research shows that only 30% of businesses know all the third parties that process personal EU data on their behalf.

According to the 2017 Verizon Data Breach Investigations Report, more than 80% of data breaches happen because of cyber criminals stealing data. But according to our survey, only 46% of businesses have deployed advanced security solutions that prevent this kind of theft. What's more, 9% of companies have no plans to deploy such a solution. In other words, they're fully exposed.

43%

of organisations currently encrypt all personal EU data, while 29% plan to before May 2018. This represents a huge shortfall. Organisations are failing to deploy solutions that help identify and protect their key assets.

33.5%

of respondents have created and communicated a data privacy policy and processing policy

30.3%

of respondents know all third parties that process personal EU data on its behalf

17.9%

of respondents have a process to test the effectiveness of data protection control

(including with third parties that process data on their behalf)

THE FINAL COUNTDOWN

Organisations seem overwhelmed. They face the potential for significant fines. They need to proactively comply. All while they navigate the ambiguity around some of the requirements.

With six months to go until the rules take effect, businesses that process EU data and have not yet started their GDPR programme must act now.

The results of our survey show that organisations are taking different approaches when it comes to GDPR readiness. But we see a sizeable disconnect between perception and reality. Businesses believe that they will be compliant with the GDPR by the May 2018 deadline. Our research and other studies suggest otherwise.

GDPR compliance is undoubtedly a complex challenge. But it need not be viewed as a burden. Indeed, 46% of organisations surveyed see GDPR as a competitive advantage—something that communicates a commitment to data privacy. Compliance helps establish trust with customers. It drives up loyalty. And it enables digital transformation in secure and compliant ways.

46% of organisations surveyed see GDPR as a competitive advantage. It communicates an investment & commitment to data privacy.

CONCLUSION

Data breaches are at an all-time high. That means the time is now to identify and protect all personal EU data and drive towards GDPR compliance. Failure to do so will lead to major business disruption.

What's more, adhering to a compliance and standards-based framework can help businesses attract and retain more customers. GDPR compliance highlights an organisation's investments in security, data privacy, and customer care. By building trust with consumers, businesses can differentiate and grow in an ever more competitive and global market.

We recommend a four-pronged approach to bridging the GDPR compliance gap:

1. **Discover and classify all personal data.**
2. **Create a plan to close all identified protection control gaps.**
3. **Protect all personal data by developing and implementing effective security controls.**
4. **Enhance security controls. Monitor, detect, respond to and report all policy violations and external threats.**

For more information on how to get your organisation GDPR-ready, visit **proofpoint.com/GDPR**

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organisations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organisations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint®

www.proofpoint.com