BearingPoint®

GDPR – your employees could make or break you

BearingPoint®

In this white paper

GDPR – your employees could make or break you

Sustainable compliance

If you have set yourself the deadline of losing 20kg in 3 weeks, you will probably have to resort to drastic measures to achieve this; be it undergoing an expensive procedure, or following the latest fad diet. However, unless you change your core behaviour and follow a new – sustainable – regime, that weight will soon come back to haunt you. For many organisations, losing 20kg in 3 weeks is what the journey to GDPR compliance currently feels like. Caught up in the rush to achieve compliance, organisations are losing sight of the need for a sustainable approach. Such sustainability will not be guaranteed with significant, one-off expenditure, but it will need to be nurtured with continued investment in workforce education.

With the 25th May 2018 deadline fast approaching, organisations are required to embark on a GDPR compliance journey which – depending on their size and data protection maturity – is most likely going to be a complicated, lengthy, and costly process. Compliance programmes tend to focus on the design and implementation of operational, legal, IT, and security measures, but to be successful, the new measures need to be carefully communicated to - and understood - by all employees. Tackled independently, these programmes can appear complex and unachievable, however, if they are underpinned by a meaningful privacy and security organisational culture, such programmes will not only ensure compliance, but will have a lasting impact.

"With the 25th May 2018 deadline fast approaching, organisations are required to embark on a GDPR compliance journey which – depending on their size and data protection maturity – is most likely going to be a complicated, lengthy, and costly process."

The soft underbelly

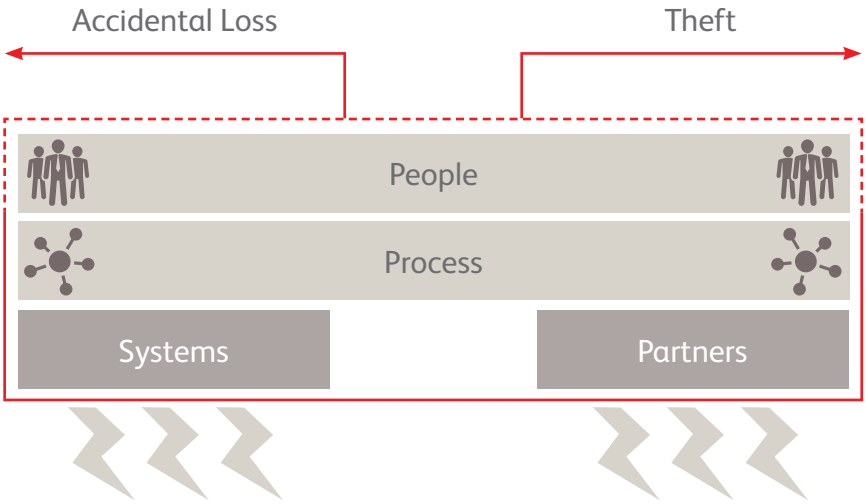
Most organisations hold a multitude of data and under the GDPR they are required to take appropriate steps to protect personal data in particular. Personal data is defined as any data that can personally identify someone, this includes employees as well as customers. Many organisations will understand this to mean ensuring that their databases have the necessary security in place, however, even with the best processes and security systems, organisations are not immune to data breaches. It is increasingly apparent that the threat is not only coming from external sources, but internal sources too. A recent survey by IT Services firm Bluesource revealed that 60% of senior IT executives view their staff as the biggest threat to GDPR compliance,[1] with many examples of internal data breaches regularly hitting the headlines to support this view.

It can be said that what is normally considered the strength of an organisation – it's employees – may in fact be its soft underbelly when it comes to data protection and compliance. Whether through unintentional action or intentional malicious activities, employees can expose organisations to litigation and liability, significant financial costs, and huge reputational risks.

what is normally considered the strength of an organisation – it's employees – may in fact be its soft underbelly

[1] https://www.bluesource.co.uk/knowledge-hub/computer-weekly-features-gdpr-survey/

BearingPoint®



it is the workforce operating, building and adhering to the compliance measures who must truly understand the purpose behind it for the benefit to data subjects to be realised, and compliance achieved and maintained.

Risks of an ill-informed workforce

One of the key purposes of the GDPR is to give control back to individuals over their personal data. However, how can you be certain that there is a genuine delegation of control – for the purposes that the regulation intended – if those influencing the key interactions and relationships with data subjects do not understand or follow the data protection rules?

New systems, security measures, business processes, and revamped customer interfaces can all achieve a degree of compliance with the new regulation, but it is the workforce operating, building and adhering to these who must truly understand the purpose behind it for the benefit to data subjects to be realised, and compliance achieved and maintained.

The risks of having a workforce ill-informed on data privacy, security and the GDPR's requirements are real. History has proven that a data breach can be as simple as personal data being included in an email, or an un-encrypted memory stick that holds personal data falling into the wrong hands. A report by Sharp Business Systems recently revealed that "one in twelve office workers has had access to confidential information that they should not have had, and 24% admitted to storing work information in the public cloud even though they are not permitted to"[1].

The consequences of a breach under the GDPR are more substantial than anything we have seen before. Fines of up to €20 million (£17.1m) or 4% of global turnover - whichever value is greater – could threaten the continued existence of those organisations guilty of a breach.

75% of large organisations suffered staff related security breach

50% of the worst breaches were caused by inadvertent human error

Type of staff related incidents:

- Unathorised access to systems or data
- Breach of data protection laws and regulation
- Misuse of confidential information
- Loss or leakage of confidential information

Examples of staff related malicious breach:

- An employee inappropriately copied and removed customer information. This breach affected around 108,000 international health insurance policies
- Employees from a 3rd party supplier gained "unauthorised and unlawful access" to personal data of over 20,000 customers
- An employee stole and sold customers personal account details to rival firms

[1] http://www.cbronline.com/news/cybersecurity/business/ignorance-isnt-bliss-gdpr-fines-loom-staff-ignore-data-policies/

It is not just financial penalties that organisations will be at risk of incurring, but the reputational damage resulting from the negative publicity associated with a breach. This was seen in October 2015 when a cyberattack against TalkTalk saw 150,000 customers' details leaked due to the organisation's inability to encrypt and store data securely.[1] The impact of the attack quickly became clear; the company suffered a £15m trading impact and extra "exceptional" costs of between £40m and £45m during the third quarter of 2015. Further to that, the company revealed that 95,000 of the 101,000 subscribers it lost during the following three months were because of the breach.[2] With global turnover of £1.795bn in 2015,[3] under GDPR TalkTalk could have seen a fine of up to £71.8m. In this case the breach was due to inadequate security measures, however, the risks are clear - organisations must take breach avoidance seriously, and increasingly such breaches are originating inside organisations.

Based on action taken by the Information Commissioner's Office (ICO) in the last 4 months, 53% of cases resulted from a lapse of data security. Of these, 70% resulted from accidental or deliberate data loss from a business by their own employees.[4] Physical and technical measures (e.g. access control) – along with robust policies – can be used to minimise malicious breaches, however, the GDPR requires a change of mindset and organisational culture to fully address these risks.

Fines of up to €20 million (£17.1m) or 4% of global turnover – whichever value is greater – could threaten the continued existence of those organisations guilty of a breach

A three-step approach

So, how do you protect against data breaches caused by employees? Whilst the risk of a breach will always exist, it can be significantly reduced by the careful implementation of an organisational culture that champions privacy and security.

Step 1. Inform

Making privacy and security a core component of organisational culture is critical to the successful implementation of any GDPR compliance programme. Introducing a comprehensive awareness and training programme which looks to improve understanding, educate employees, and change their behaviours, will compliment other GDPR compliance initiatives and give them longevity. Bringing GDPR in to your organisational consciousness will help to embed a privacy first culture, sustaining compliance in the long-run.

1. INFORM

The quick and easy step is to inform employees of the requirements introduced by the GDPR and the new processes or systems implemented as part of the organisation's compliance programme. However, employees must also be educated on data privacy and security – highlighting the consequences of their actions, and ultimately change their behaviour and mentality when it comes to handling personal data.

Step 2. Train

Embedding a privacy and security culture cannot be achieved by carrying out a series of one-off activities. As well as generic awareness training for all employees, tailored briefings and training should be aimed at specific sections of the workforce to achieve short and long-term impacts, for example;

- Executive and senior management – brief on the GDPR impact to their specific functional areas
- Operational Teams – focus on the personal data handled by teams; empowering them to embrace and drive new business processes
- Design and Development Teams – implement new design frameworks which stress the importance of minimising the spread of personal data within an enterprise, isolating storage and use of personal data to specific parts of the organisation.

2. TRAIN

[1] https://www.theguardian.com/business/2015/oct/30/talktalk-hackers-accessed-fraction-data-cyber-attack
[2] http://www.wired.co.uk/article/talktalk-hack-customers-lost
[3] TalkTalk Annual Report 2015 - https://www.talktalkgroup.com/dam/jcr:04037e42-6a6d-4fcf-9bea-8f339240d0ba/Annual%20Report%202015%20Final.pdf
[4] https://ico.org.uk/action-weve-taken/

BearingPoint®

3. EMBED

Step 3. Embed

Compulsory training courses alone will not be sufficient to maintain awareness and change the culture, instead, employees should be continuously reminded of their obligations and best practice. To facilitate this, organisations may consider setting up a Privacy Centre of Excellence, nominating a privacy and security champion in every department, issuing regular newsletters, organising annual events, and making privacy and security part of their employees' personal objectives and performance review process.

To be effective, the awareness and training programme needs to be embraced by the leadership team and senior management. Ultimately, it is the leadership who have the power to build privacy into the core mission and values of the organisation. Endorsement from the leadership team will elevate the importance of data privacy in the organisation and help to embed a lasting 'privacy and security first' culture.

Stand out

The benefits of having an embedded data privacy and security culture reach further than reducing the risk of a breach and the resulting financial penalties. In much the same way, as deciding whether to set off on a sustainable weight loss path, or choosing to invest in costly surgery, the GDPR represents a fork in the road where organisations can seize the opportunity to educate and empower their employees, instilling a 'customer first' attitude throughout the business, with lasting benefits.

Employees who understand the importance and remit of data privacy are more willing to follow (and to help mould) processes that are conducive to data protection and security. In turn, they will develop products, services, and a customer experience with data privacy at the core. In the event of a data breach, privacy conscious employees are more likely to be proactive and nurture the principle of 'Privacy by Design' – a key principle of the GDPR.

As the GDPR elevates the status of data protection in society, it is those privacy conscious organisations who will differentiate themselves; avoiding security incidents, litigation, financial losses, and reputational damage – but also increasing trust with their customers and boosting loyalty. Just like those who choose the sustainable path to weight loss, the organisations who choose a holistic and sustainable approach to GDPR compliance will profit in the long term.

Employees who understand the legislation, who respect data privacy, and understand the risks if they don't, will provide your organisation with the foundations from which to build and embed an exemplar GDPR compliance programme.

Contact

Authors

Aloke Kapur, Partner
aloke.kapur@BearingPoint.com

Dr Baljit Sarpal PhD, Managing Director, Sarpal Consultancy Ltd
baljitsarpal@sarpalconsult.com

Writing Team

Capucine Nivet, Senior Consultant
capucine.nivet@BearingPoint.com

Joe Barrs, Senior Business Analyst
joe.barrs@BearingPoint.com

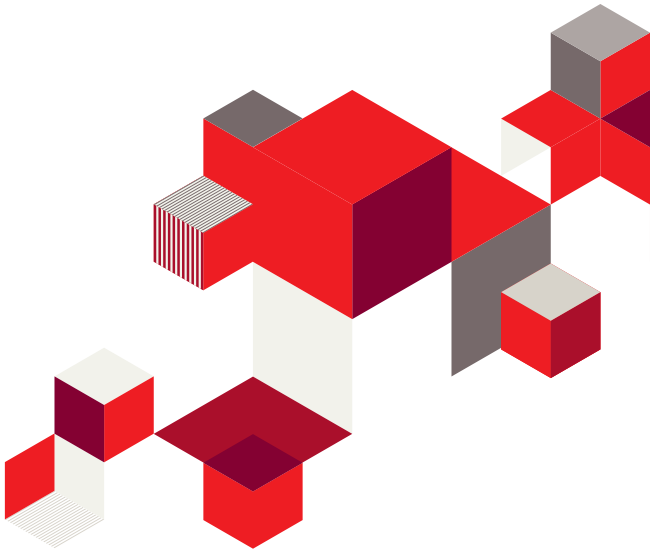
BearingPoint®

Committed consultants with adaptive intelligence

BearingPoint consultants understand that the world of business changes constantly and that the resulting complexities demand intelligent and adaptive solutions. Our clients, whether in commercial or financial industries or in government, experience real results when they work with us. We combine industry, operational and technology skills with relevant proprietary and other assets in order to tailor solutions for each client's individual challenges. This adaptive approach is at the heart of our culture and has led to long-standing relationships with many of the world's leading companies and organizations. Our 3350 people, together with our global consulting network serve clients in more than 70 countries and engage with them for measurable results and long-lasting success.

For more information, visit our website www.bearingpoint.com.

BearingPoint®



BearingPoint
Aloke Kapur
Partner
UK
T +44 20 7337 3160
E aloke.kapur@bearingpoint.com

www.bearingpoint.com