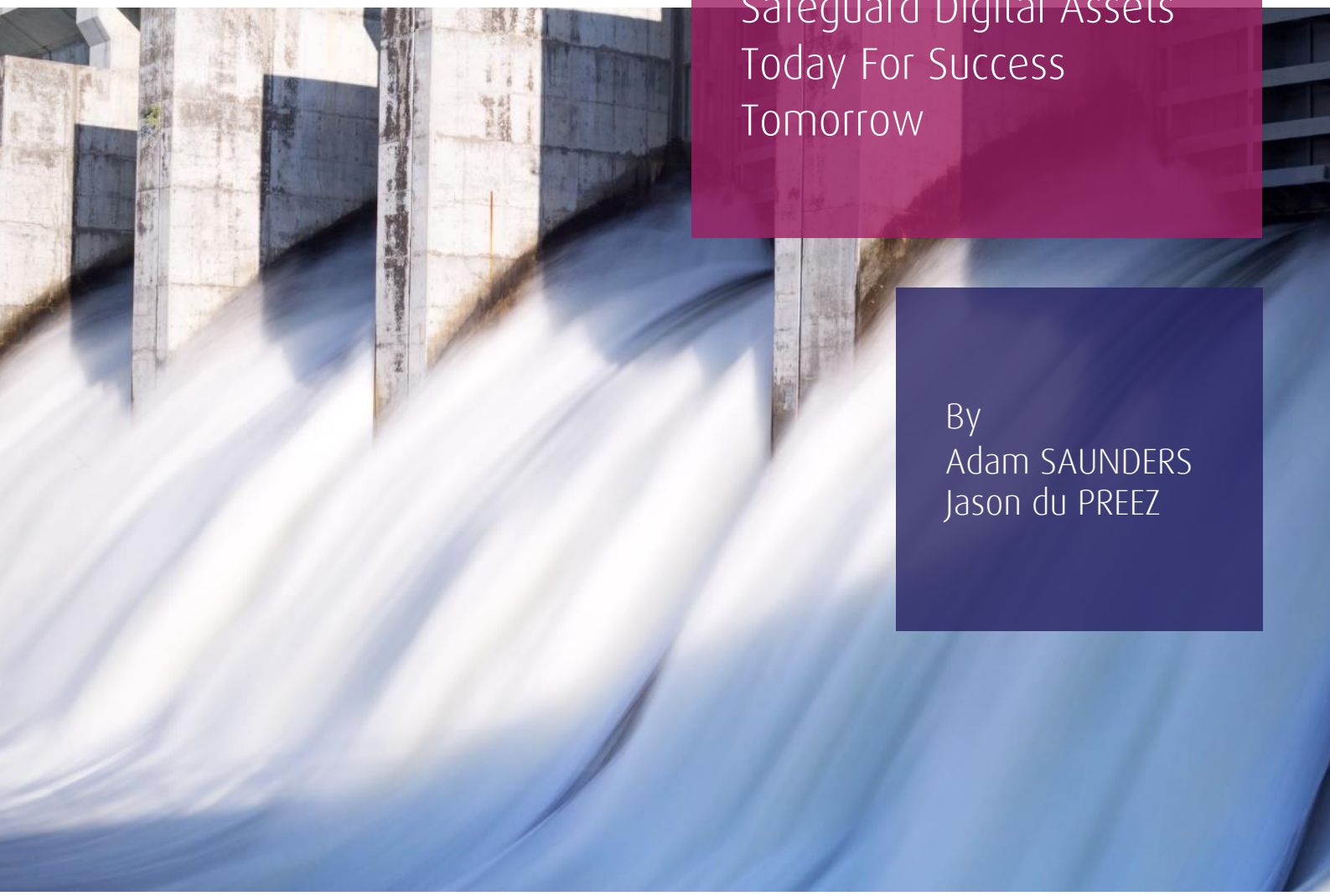
Digital Leadership

# Cyber Security

## Data Privacy
How Boards Can Safeguard Digital Assets Today For Success Tomorrow



By
Adam SAUNDERS
Jason du PREEZ

PRIVITAR

Amrop
Leaders For What's Next

# Cyber Security

## Data Privacy: How Boards Can Safeguard Digital Assets Today For Success Tomorrow

Cyber continues to dominate headlines - and rightly so. Not only is the topic wide-ranging, but cyber attacks are mushrooming daily, unconstrained by geographic or sectoral borders. Like so many of today's business issues, human decision-making and behavior lie at the heart of the problem. How can companies develop digital offerings without inviting the real threat of cyber risks? Beyond the numbers, how much insight do boards really have? Within board governance, what data governance structures are needed?

These are just some of the questions that inhabit the cyber security landscape. In this series, Amrop breaks the subject into bite-size portions. In this first piece we delve into the fast-evolving world of privacy engineering – the tools, technologies and processes that can be used to enforce privacy policies to deliver the principles of privacy by design, considering privacy risk throughout the entire data life cycle.

With a focus on Financial Services (one of the top three sectors to suffer customer defections after a breach) we asked executive and non-executive board members to reflect on the issue. Their input confirms that cyber security is top of the board agenda for data-centric businesses.

### Setting the Scene

By Adam Saunders
*Leader, Global Financial Services Practice, Amrop*

In this Cyber Security series, Amrop collaborates with some of the industry's most innovative companies as they trailblaze through the digital landscape. This first insight piece is co-authored with Jason du Preez, CEO of Privitar, a leader in the development and adoption of privacy engineering technology.

**Let's first set the scene for our series. Accumulating evidence suggests:**

1. The cost of data breaches is on the rise
2. The biggest loss to organizations remains the erosion of business
3. Boards and CEO's are increasingly held responsible for data breaches – and penalized accordingly
4. Well-resourced governments are increasingly suspected of targeting companies or influencing the affairs of other states
5. Companies are switching on to cyber security, investing in speeding up detection of data breaches and their escalation to top management
6. There is a direct correlation between data governance and the cost of breaches
7. The Internet of Things and machine learning offer exciting new ways to protect systems and detect attacks. However they may also make attacks more efficient – and allow new types of attack.

Now is the time to put privacy at the top of business agendas. Complying with the regulation is something we're preparing for, alongside every other organization around the world that handles EU citizens' data."

Kevin Ellis
*Chairman, PwC*

Human error is the most common factor in a data breach. However, deliberate cyber attacks are evolving and are increasingly becoming a commoditized form of criminal activity. Once the domain of the technically-minded, off-the-shelf cyber attacks can now be bought on the black market by anyone wanting to do so. Formerly a broad and blunt tool for mass disruption, they are becoming ever more sophisticated and tailored, designed to target and exert maximum pressure on people, departments or organizations. And as we move our businesses - and our lives – further into the digital plane, they are set to expand.

Against this backdrop, organizations must tackle the tension between two forces. On one hand, digital innovation for automation, new revenue streams, operational efficiencies (wins). On the other, given the exposure such innovations build into the business, protection against significant potential risks (losses). Central to both is data. This is one of the most precious assets a company can own in terms of its value to reveal, anticipate and respond to customer habits and needs, and opening up new marketplaces. It is also its most vulnerable asset.

For companies looking to extract value from advanced analytics, machine learning and sharing with third parties, digital information has become a major strategic asset. Burgeoning volumes of it are now being amassed, much containing proprietary and highly sensitive data. Employee records, banking transactions and trade data are just some examples.

But every asset has its price. Growing concern for customer privacy is restricting access to sensitive information and proving a barrier to innovation.

Incoming GDPR regulation which calls for 'privacy by design' will put further compliance pressure on firms. The era of the Data Protection Officer (DPO) is upon us, and one of his or her key functions is to ensure customer privacy.

At Barclays we consider it a critical duty to protect the data which our customers and clients hold with us. We believe the quality of a bank's security, which is intrinsically linked to trust, can be a sustainable and strategic point of service differentiation today."

*John McFarlane*
*Chairman, Barclays PLC*

## The Ripple Effect of Data Breaches

The recent breach of social network site MySpace is a prime example of a case where harm could likely have been avoided by robust privacy engineering. It also demonstrates the role played by online market places in breached data. In May 2016, motherboard.vice.com cited an *'oft-repeated adage in the world of cybersecurity. There are two types of companies, those that have been hacked, and those that don't yet know they have been hacked.'*

According to motherboard.vice.com, MySpace apparently belonged to the latter category. The data hack was based on a previous, unreported breach.

Only the week before, Peace, the hacker, had been busy selling the account information of 117 million LinkedIn users, including emails and passwords, stolen during the LinkedIn breach of 2012. The paid hacked data search engine LeakedSource also claimed to have obtained the data.

Peace claimed to be in possession of over 360 million emails and passwords of Myspace users, putting the data up for sale on the dark web market The Real Deal with an asking price of 6 Bitcoin (around $2,800).

If the total numbers were accurate and the data indeed came from MySpace, this would be one of the largest data thefts ever, according to motherboard.vice.com.

## What did MySpace miss?

LeakedSource said that the passwords were originally "hashed" with the SHA1 algorithm – one that is known to be weak and easy to crack. Furthermore, MySpace failed to 'salt' the passwords – 'adding a series of random bytes to the end of passwords before hashing them to make them harder to be cracked.' LinkedIn had similarly failed to do so.

"Insurance is the business of trust. You are trusting that when something goes wrong, when you probably need help the most, that your insurance will make sure you recover. This trust is not just between the consumer and the insurer, but also necessary between brokers, loss adjustors and other claims handlers."

Richard Ward
*Chairman, Cunningham Lindsey, Member of the PRA Practitioner Panel, Bank of England*

Data privacy is a major part of our proposition and is central to our success. Policies alone don't provide the reassurance and confidence which customers demand. Users should experience it as part of their relationship with the company...

## Data breaches take a toll at the top

Beyond their toxic effect on customers (arguably a societal responsibility issue), the fallout of data breaches can inflict serious damage on the people at the helm of organizations, with repercussions far beyond the ICT function.

In 2015, the UK telecommunications challenger TalkTalk suffered a cyber-attack that cost it £60 million, 101,000 customers, and a record £400,000 fine from the Information Commissioners' Office (ICO). Information Commissioner Elizabeth Denham was unequivocal: "TalkTalk's failure to implement the most basic cyber security measures allowed hackers to penetrate TalkTalk's systems with ease. Yes, hacking is wrong, but that is not an excuse for companies to abdicate their security obligations."

In February 2017, TalkTalk's CEO Dido Harding announced that she would step down, insisting that her departure was unlinked to the cyber-security incident. This was, she said "ancient history, [there is] no connection at all".[2]

... that's why data security and privacy impact almost everything we do, from internal procedures to customer service, technical security, product development and marketing. If you get it right, customers should feel certain that their data is properly handled and secured in every interaction with your business."

Robert Glynne | *CEO, BullionVault*

The following March it was widely reported that Marissa Mayer, the outoing Chief Executive of the beleaguered Yahoo, would take a pay cut "after a board investigation found that she and other senior executives failed to "properly comprehend or investigate" a 2014 security breach.[3,4]

A 2013 data breach at US retailer Target was at least partially responsible for the board's request for CEO Gregg Steinhafel's resignation, according to industry observers. "The data breach was the last straw," said Bloomberg[5]. The CIO was also duly replaced. Nor did the buck stop there. According to Forbes: "The Target board of directors was also under significant pressure. A proxy firm, Institutional Shareholder Services, had recommended that investors oust seven board members. The firm said the board failed to protect the company from last year's data breach. The board members were able to convince shareholders to re-elect them, however, although the message to them was clear that future data security breaches were considered to be their responsibility."[6]

# An Insider's Guide to Data Security

By Jason du Preez | *CEO, Privitar*

Breaches are most often caused by insider action – whether accidental or malicious. At the same time, a new market has emerged for personal and sensitive data, incentivising criminals to buy cyber-attacks against companies. In this section, we give strategists a technical apéritif to some of the key measures that can be taken to counter the problem.

Whilst cyber security measures protect data from unauthorized access, privacy engineering tools can protect sensitive data *when* it is accessed. Indeed, security and privacy engineering should be thought of as complementary fields which together deliver data protection.

Privacy engineering incorporates a range of techniques which make sensitive data less vulnerable to exploitation. It allows data controllers to select an acceptable level of privacy risk, taking into account the trustworthiness of the stakeholders and environment involved. The tools can protect sensitive information at the point of access whilst preserving the valuable patterns and relationships in the data. This gives companies the best of both worlds - the ability to innovate *and* use data safely.

## Breaking Links

One method is to apply a privacy policy to sensitive data and create an anonymized copy. Identifying fields are tokenized or encrypted. The rest of the data is then perturbed to prevent re-identification via linkage attacks - attempts to re-identify individuals in an anonymized dataset by combining that data with another dataset. The 'linking' uses indirect identifiers also known as *quasi-identifiers* - pieces of information that are not themselves unique identifiers, but can become identifying when combined with other quasi-identifiers. For instance, an individual's date of birth and postcode are quasi identifiers; each one alone is not sufficient to identify an individual, but in combination they usually are.

## Example use case | Leveraging public cloud

Although the cost per bit of data storage and processing is going down, volumes are rapidly increasing, making data infrastructure a significant cost.

Many look to the cloud as a cheaper and easier way of managing resource, but are held back by concerns over data protection. For these companies privacy engineering offers a way of managing, reducing or removing the associated risk, allowing them to safely leverage public cloud infrastructure, and so reduce costs and increase efficiency.

Information such as salary, transaction history, overdraft limit, location data and many others are examples of quasi-identifiers.

To resist a linkage attack, the quasi-identifiers in a dataset must be transformed to achieve what specialists call *k*-anonymity. This means that even when someone has auxiliary information, each record is still indistinguishable from at least *k*-1 other records.

The *k*-anonymity approach is useful for:

- System development and testing
- Analytics, data science and machine learning
- Sharing with third parties
- Processing in cloud environments

An alternative method is to prevent direct access to the raw data itself by using a privacy preserving interface, from which users can submit queries.

This ensures that usage is subject to strict authentication and access control, and all queries are logged and audited. Importantly, Noise Addition (essentially adding or multiplying a randomized number to confidential, quantitative attributes), prevents users from extracting private data, ensuring differential privacy, with further protection provided by behavioral analytics for attack detection.

This privacy preserving interface approach is particularly useful for sophisticated analytics or new data products.

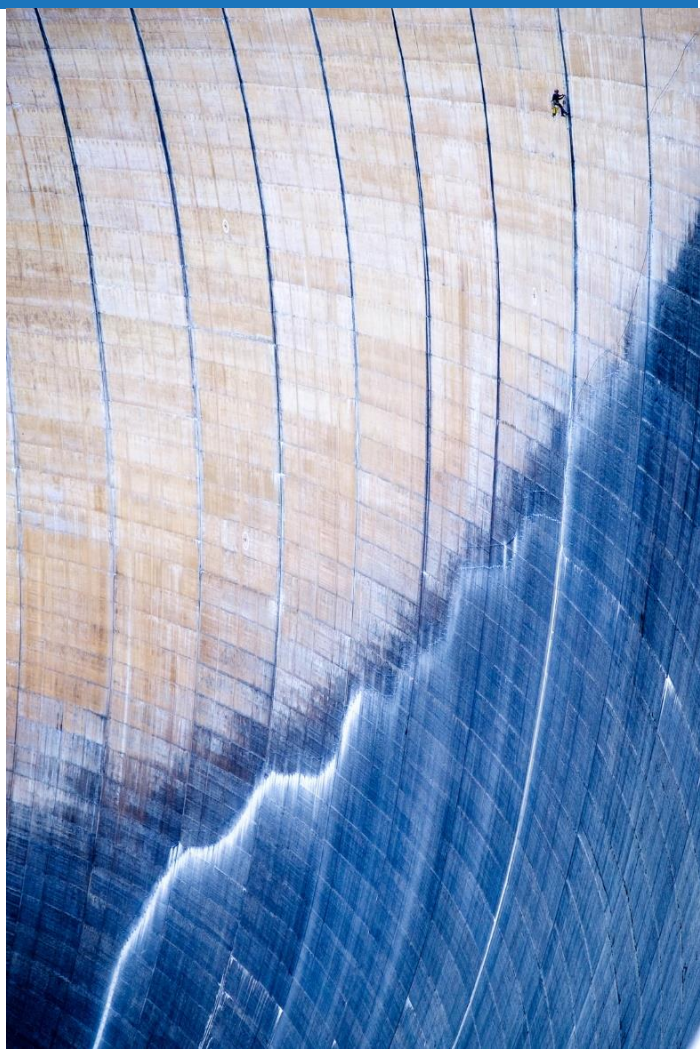
## General Data Protection Regulation (GDPR)

All organizations handling personal data must be compliant with the new GDPR by the 25th May 2018, or face fines of up to 4% of their global revenue.

The GDPR aims to pave the way for the digital economy of the future by establishing the rights of individuals and the responsibilities of those handling their data. Amongst other changes, it mandates Privacy by Design principles; a foundation of privacy engineering.

"Companies need to understand that in a data breach situation they will be judged on an ex-post basis and will need to demonstrate that they had done all they could to prevent it – regardless of whether they technically had responsibility for data security. Boards need to ensure they have taken that into account as part of their governance role."

Jerry del Missier |
*Founder and Executive Chairman,*
*Copper Street Capital*



The potential (and often all-too-real) repercussions of a lax approach to data privacy mean that senior executives have a clear and present responsibility to ensure a better approach across the organization.

The principle of responsibility will be enforced with the introduction under the GDPR of the Data Protection Officer (DPO) who should be appointed by all companies whose core business operations involve large scale, regular and systematic monitoring of data subjects, or the large scale processing of sensitive personal data[7]. The DPO must report to the highest management board and will be responsible for ensuring that the organization is compliant with data protection law.

The International Association of Privacy Professionals (IAPP) estimates that this will lead to 75,000 new DPOs globally. Whilst an IAPP certification is not required to be a DPO, it is emerging as the dominant relevant certification. This could lead to a shortage of DPO's, as there are currently only about 8,000 IAPP certified professionals worldwide.

Further research by the IAPP and TRUSTe found that around 90% of organizations would be looking to appoint a DPO from staff internally.

One has to ask whether these internal hires will really be able to make the changes required under the new legislation. Like compliance before it, is this approach really addressing the problem or paying lip-service to the role?

Whilst the DPO will be integral to an organization's approach to privacy, and may own it, DPOs and CDO/CIOs need to work together on organizations' privacy engineering strategies.

Privacy by design, as mandated in the GDPR, promotes the incorporation of privacy and data protection compliance in the early stages of any project and throughout its lifecycle. This means that certain roles within the company will have specific responsibilities in addition to those held by the DPO, CDO and CIOs, as indicated in the matrices overleaf.

## Digital Leadership Matrix

**Board** - responsible for setting overall digital strategy, managing reputation, risk and ethics.

**CDO and CIO** - work together on privacy engineering strategies.

**DPO** – Under GDPR regulation, a compulsory role for companies with personal data as their core business, ensuring compliance with data protection law. The DPO is responsible for data protection compliance.

| Analysts and data scientists | Legal & compliance specialists | Data engineers |
|---|---|---|
| Will need to be able to access data securely, and to understand and control how best to apply privacy engineering techniques to maximise data utility. | Will want to have confidence that the organization is meeting and exceeding compliance regulation. | Will be required to build privacy protection into the data platform at each stage of the data pipeline. |

## Digital Competency Matrix

**Board** – ideally integrate a digital/technological Non-Executive Board Member, whose role is to catalyze and guide in critical areas[8], including cyber security and data privacy. At minimum, ensure his or her input to board meetings and the board agenda in either live or written form. Assign a dedicated Strategy Day to connect the Board and Executive Management on the digital/technical theme – outside the boardroom. Install a formal coaching system – regular sessions between a board and Executive Management team member (CDO, CIO, or DPO).

**CDO and CIO** – A 'T-shaped' profile – hands-on experience of IT culture change, plus a broad, ideally international, track record in areas such as digital disruption, accelerating innovation, and fine-tuning customer-centricity[8]. Must have a clear perspective on managing online security risks.

**DPO** – expert knowledge of data protection law and practice, enabling him or her to deal effectively with all data protection matters in a timely way. S/he must inform and advise relevant stakeholders (controller, processor, employees processing personal data) on GDPR obligations, and monitor compliance, adopting an advisory and consultative role.

# Conclusion

## Innovation and Safety Go Hand-in-Hand

The world is painfully waking up to privacy risk. As ever more personal information is collected, the threat to the privacy of individuals is intensifying, and customers are increasingly aware of the risks of handing over their data. This means that it is imperative for boards to install the tools, technologies and processes that will not only assure data protection, but help their organizations maintain a watertight reputation for that protection. More than a question of risk or reputation management, data security is a lynchpin of organizational evolution. Innovation is catalyzed by access to the insights sensitive data provides. Lose public trust, and the evolution of a company may be compromised.

If it is critical to be transparent about how you protect (and use) private data, so, too, is doing things with purpose. This means being clear about what data you might need in the future, rather than gratuitously storing personal data that have little or value for your organization. It means putting the right tools in place to enable data-driven innovation whilst protecting personal information.

| Board Agenda: 5 Steps to Embed Privacy into the DNA of Your Business. | |
|---|---|
| 1 | Ensure the CIO or CDO has a clear view of the sensitive data held by the organization, and what is currently being done with it. |
| 2 | Consider and agree upon the data needs of the business – these could include data science/analytics, innovation, development and testing, IT, research – the key is to understand who will need access to the data, and to what level. |
| 3 | Assess and define privacy policies -This will generally be the responsibility of the legal team, or DPO, working closely with the CIO or CDO. |
| 4 | Apply technical controls to mitigate privacy risk, and to bring consistency and full accountability to the governance of confidential data. |
| 5 | Train teams about the privacy risks when handling sensitive data, and how best to manage those risks. |

Preserving your customer's right to privacy and the protection of their data will be a clear competitive differentiator for the data-driven companies of the future.

## About Amrop

With over 70 offices in more than 50 countries, Amrop provides services in Executive Search, Leadership and Board Services. It is the largest partnership of its kind.

Amrop advises the world's most dynamic organizations on finding and positioning Leaders For What's Next: top talent, adept at working across borders in markets around the world, helping companies address digital talent leads via its global Financial Services/FinTech, and Technology & Media Practice Groups. Adam Saunders leads Amrop's Global Financial Services Practice.

**www.amrop.com**

## About Privitar

Privitar is an enterprise software company headquartered in London, with a global client base across North America, Europe and Asia.

Privitar is leading the development and adoption of privacy engineering technology enabling customers to innovate and leverage data with an uncompromising approach to data privacy.

**www.privitar.com**

## Sources


1 Hacker Tries To Sell 427 Milllion Stolen MySpace Passwords For $2,800, motherboard.vice.com, May 27, 2017
2 TalkTalk chief executive Dido Harding to step down, The Guardian, 1 February 2017
3 Yahoo hack: 1bn accounts compromised by biggest data breach in history, The Guardian, 16 December, 2016
4 Yahoo CEO Mayer Loses Bonus and Lawyer Resigns on Security Breach, Nasdaq/RTT News, March 01, 2017
5 Target Replaces Steinhafel After Breach Serves as Last Straw, Bloomberg, May 5, 2014
6 Target CEO Fired – Can You Be Fired If Your Company Is Hacked? Forbes, June 15, 2014
7 Unlocking the EU General Data Protection, 2016, White & Case LLP
8 Digitization on Boards 2016, Amrop