Dealing with the new EU General Data Protection Regulation

Time to take a fresh look at your data security.

Security as an enabler

As the digital world continues to grow, more people are paying close attention to what happens to the data they own and generate.

Smartphones and tablets have already changed the way we perform many everyday activities, like shopping and banking. But smart cities using Big Data and the Internet of Things (IoT) are about to change the way everyone interacts with the world — creating and distributing new and expanded streams of information. The digital transformation taking place in our society is a positive step forward, but will only be successful if organisations can guarantee the right to privacy through the protection of personal data.

Organisations need the right security tools and processes in place to prevent loss, theft or unauthorised access to their service users' data. Data security is vital in today's digital economy. It's the number-one enabler, allowing organisations to build public trust and confidence. Conversely, poor security is a disabler, and will undermine all efforts towards digital transformation.

A new regulation — a new opportunity.
In Europe, EU institutions have paid attention to citizens' demands for greater data protection. That's why, on 14 April 2016, the European Parliament adopted a new regulation that will replace the 1995 Data Protection Directive.

The EU 2016/679 regulation (also known as the General Data Protection Regulation or GDPR) covers the protection of natural persons with regard to the processing of personal data, and the free movement of such data. It comes into force next year and will give citizens of EU countries greater rights over their personal information, and place greater obligations on organisations to protect this data. It includes the right to be forgotten, the right to know when personal data falls into the wrong hands (e.g. hackers) and the need for explicit consent (in certain cases) prior to processing personal information.

The Digital Single Market

The unification of data-protection requirements is not the only field in which the EU has started to harmonise different legislations. The Digital Single Market is an overall strategy for Europe to create an innovation-friendly environment through three policy areas:

- Improving access to digital goods and services.
- Creating an environment where digital networks can prosper.
- Driving growth with digital technology.

As part of this overall strategy, the European Parliament will adopt the Directive (EU) 2016/1148, known as the Network and Information Security (NIS) Directive. The aim of the NIS Directive is to ensure secure, continuous operation of digital-service providers and essential services in different sectors. Local legislations in member states will contain identification of specific operators and detailed security requirements related to network information security.

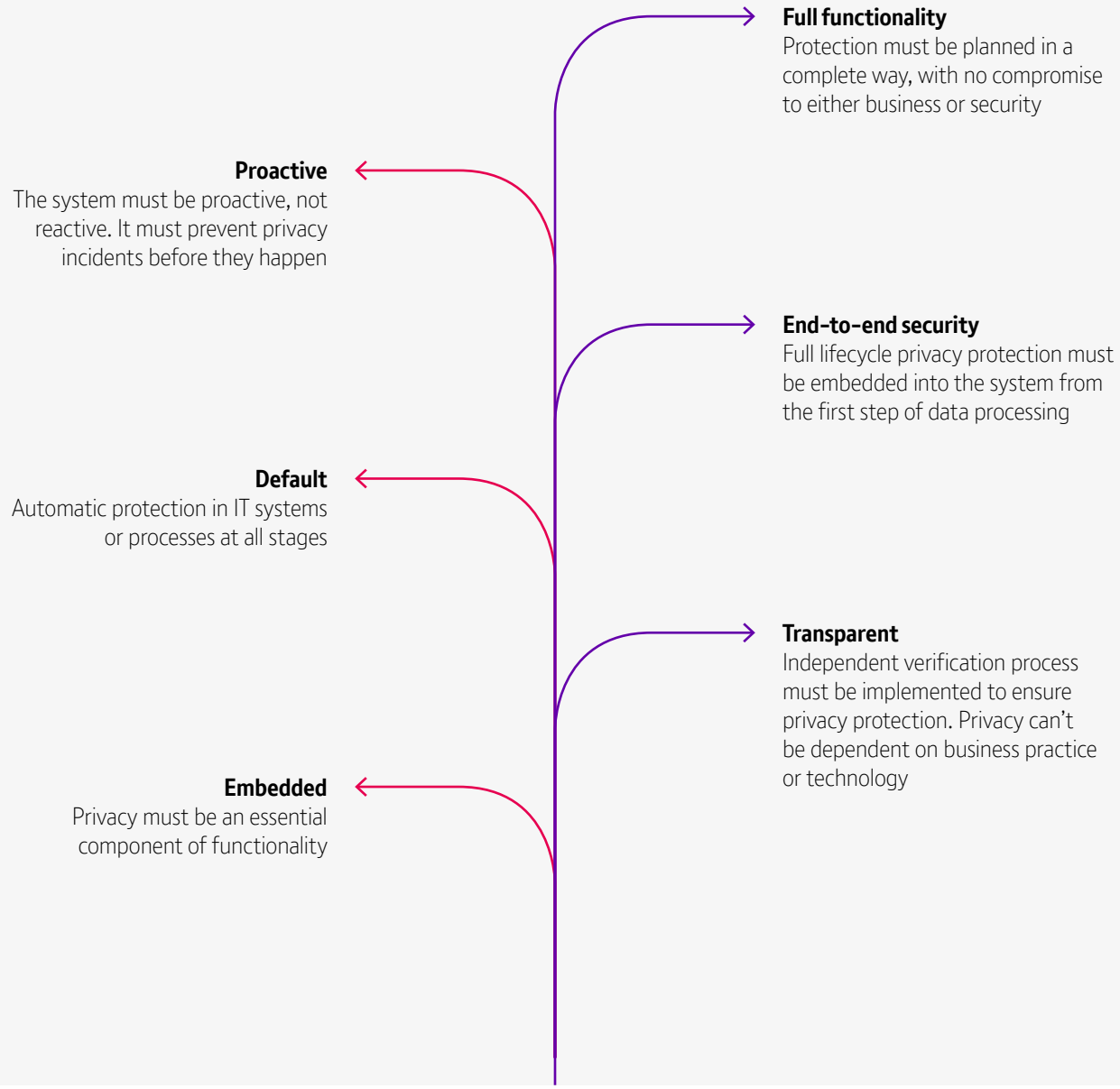
Data protection

Already a good practice requirement, GDPR requires data protection (or privacy) "by design and by default" as a legal obligation.

To comply with this, organisations must embed data protection at every level of their enterprise and incorporate it into their processes. It means they have to take privacy into account throughout the whole lifecycle of any activity, to minimise privacy risks and avoid infringing data-protection rules.

To achieve this, a combination of detective, preventative, proactive and reactive security controls are needed. Every process, IT application, and area of infrastructure has to revolve around protection of privacy.

Recommended principles: data security controls.



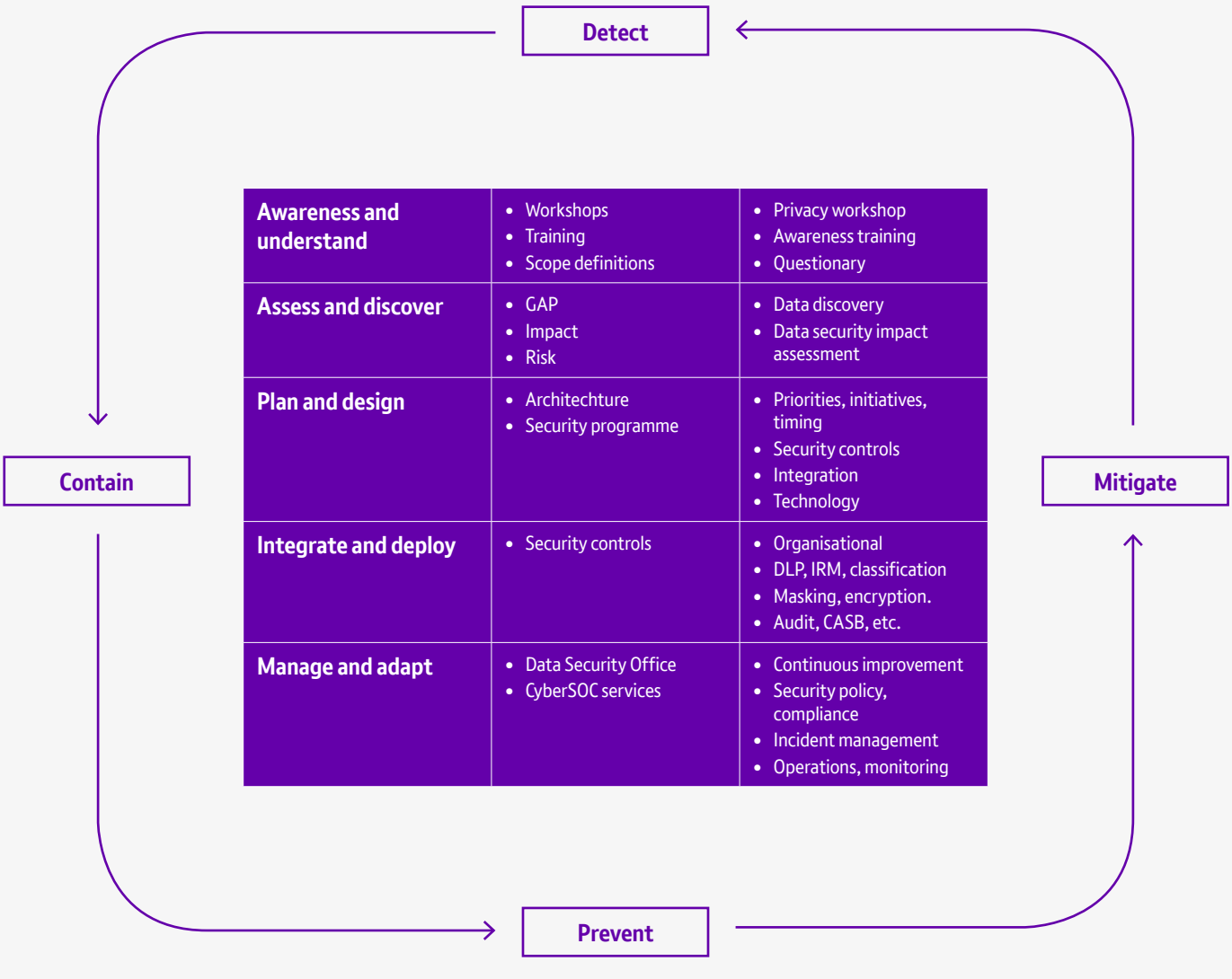
Organisations have to adapt

Organisations have less than two years left to get to grips with the GDPR, so now's a good time to ensure that they meet security requirements imposed by current laws and regulations.

The new regulation has a number of implications, for instance, it introduces stiff penalties for non-compliance which could result in fines of up to four per cent of an organisation's global annual turnover. And achieving compliance requires more than putting a new process or piece of technology in place.

Organisations have to look at their entire security landscape, because it underpins their efforts to understand and protect their data, and to comply with various legal, regulatory and industry requirements. Without a successful security strategy in place, organisations will suffer the financial, regulatory and reputational consequences that follow a serious data-security breach.

Privacy Shield Framework



Awareness and understand	• Workshops • Training • Scope definitions	• Privacy workshop • Awareness training • Questionary
Assess and discover	• GAP • Impact • Risk	• Data discovery • Data security impact assessment
Plan and design	• Architechture • Security programme	• Priorities, initiatives, timing • Security controls • Integration • Technology
Integrate and deploy	• Security controls	• Organisational • DLP, IRM, classification • Masking, encryption. • Audit, CASB, etc.
Manage and adapt	• Data Security Office • CyberSOC services	• Continuous improvement • Security policy, compliance • Incident management • Operations, monitoring

So, to adapt existing security infrastructure and ensure data is secure, organisations need to:

- gain a thorough understanding of how data moves around their organisation (and the associated processes)
- have a specific workstream dedicated to security review (gap analysis and assessment) within their data-protection programmes
- address gaps and (where necessary) redesign security architecture
- implement technical and organisational security controls, including the development of security processes to detect and mitigate data leaks.

It doesn't end there, though. Monitoring and security are ongoing processes that organisations need to stay on top of to protect data and meet regulatory requirements.

The threats to your data

Privacy laws and regulations, as well as customers and regulators, have a zero-tolerance approach to data breaches. It doesn't matter if the breach was accidental or malicious — every organisation has a responsibility to protect its personal data.

Here are the three important data-security challenges to look out for:

- **Accidental data leaks**
  This is one of the most frequent sources of security breaches. And all it takes is for an employee to type the wrong email address or leave a smartphone in a taxi. A strong internal security policy is necessary, but it still might not be enough to avoid fines of millions of euros for a simple accident (and subsequent damage to reputation).
- **Disloyal employees**
  We've seen situations in the past where disgruntled employees have taken advantage of weaknesses in internal processes and controls to take revenge against their organisation. Orginisations need to have a solid data-access policy, data-classification tools that restrict access by user profile, identity and access management controls, and cyber-intelligence services to minimise this risk.
- **Cyber crime**
  This is an ever-increasing concern for organisations. The theft of personal information, using tools such as targeted malware, has become a profitable cyber crime. Organisations have to make sure their cyber defences can prevent data from falling into the wrong hands. An end-to-end approach is essential — each company has to protect against all potential risks, but a cyber criminal only needs a single weakness to find a way in.

Securing new opportunities

Organisations have plenty of work to do to get their security up to scratch

But this doesn't mean they have to view data-protection requirements through the prism of punitive measures alone. While data protection is something organisations already have to comply with, the new regulation offers an opportunity to review and redesign their security strategies in a way that protects data against new and existing threats, and builds a strong brand based on public trust.

In the same way that safety is a prime consideration for people purchasing a product in the physical world (a car perhaps), in the digital world, public service users see data security as a key factor in their decisions. If people associate security with public services, there's a good chance that the transformation of services and shift to digital delivery will be successful and efficient.

Dealing with the data

Another way for organisations to get a better return on compliance activity is to extend security processes to other critical areas of business. Current and upcoming privacy laws only cover protection of personal information. But organisations can equally apply the architecture and controls they use to comply with these laws and regulations to protect other confidential information, such as intellectual property, and avoid the risk of losing valuable research and development information to a security breach.

Privacy by design and by default

Currently a good practice requirement, a cornerstone of the GDPR (impacting areas such as product development, product launches and business change) is the principle of "privacy by design and by default".

This stipulates that — from the initial stages onwards — organisations must consider the impact that processing personal data can have on an individual's privacy. It means, for example, that every new business process or product that could involve personal data or impact the privacy of an individual, must be designed in accordance with data-protection requirements. Within the assessment, particular attention must be given to the technical-security controls required to protect the data.

Organisations need to adopt a standardised data-security process that complies with the new legislation and allows them to easily build required security controls into new products and services.

GDPR essentials

Organisations now have less than two years to prepare for the GDPR, so here are the basics they need to know about this new EU regulation

Scope
The new data-protection regulation — like the current DP Directive — affects all industries and organisations that process the personal data. It's also applicable to both public and private sectors.

Timings
With its publication in the Official Journal of the EU, the regulation will come into effect on 25 May 2018.

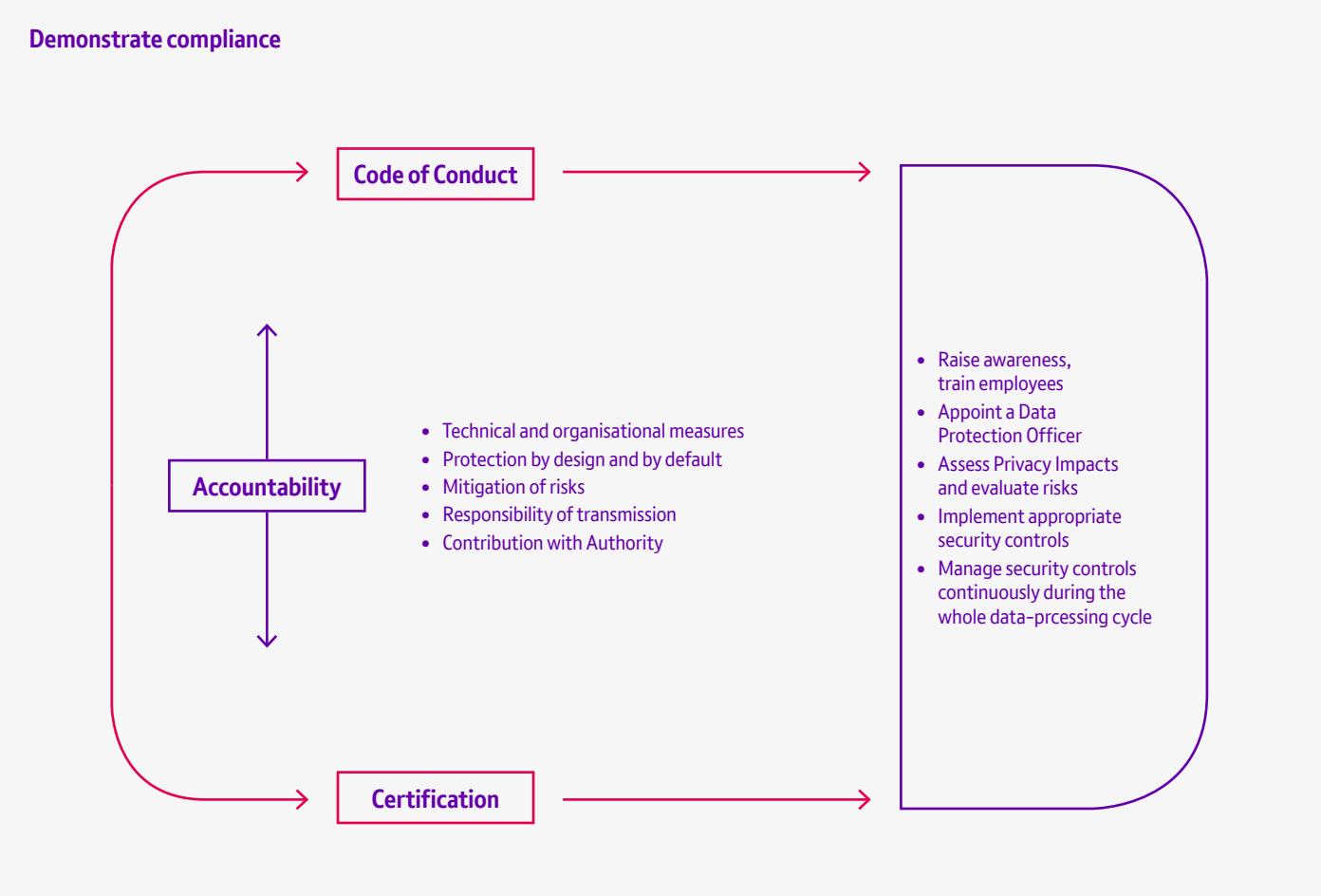
Penalties
In the event of a compliance breach, supervisory authorities can impose fines of up to four per cent of an organisation's worldwide annual turnover, or €20 million — whichever is higher.

Notification of data breaches
Organisations have to notify their supervisory authority within 72 hours of any data breach, and they may also have to notify their customers.

Data Protection Officer (DPO)
In certain cases GDPR requires organisations to appoint a DPO. A DPO must be an independent person who reports directly to management and has the responsibility to highlight any issues or concerns around the organisation's data protection compliance. Appointing an experienced data protection professional to head your data protection compliance, even if not legally mandated, is good practice and can be an effective way of demonstrating accountability.

Rights of the citizens
Anyone who deals with a European controller will have the right to access and rectify their data, the right to be forgotten and the right to be informed about the purpose of any processing their data requires.

Data security
As per existing regulations, organisations have to ensure they have technical and organisational security controls in place to guarantee the safety of any data they process. The GDPR is a good opportunity to review and tighten these controls.



Technical challenges to watch out for

Cloud computing
Many organisations have already turned to the cloud, either for their own internal use or to meet customer demand. Most do, however, have concerns regarding the lack of control over underlying IT infrastructure used in cloud services — especially when it comes to sharing data centres with companies and competitors who have diverse risk profiles.

Of course, choosing the right cloud provider and agreeing the contractual terms to manage security is fundamental. But these aren't the only steps organisations need to take to protect their data in the cloud. Controls such as information rights management (IRM), cloud access security brokers (CASB) and cloud data-loss prevention (CDLP) can offer the same (or better) security than on-premises solutions, if designed and implemented correctly.

Big Data
Big Data allows organisations to model and anticipate customer and market behaviours, giving them greater insight during the decision-making process. The security of data is key because the sheer volume of data means that the scale and impact of a potential breach would be significant.

Privacy considerations around Big Data are complex and, to minimise the risk, organisations need to draw on a wide-range of advice, from architectural and technical to more strategic consultancy.

Shadow IT
Shadow IT can mean that employees are accessing unauthorised applications and systems, and is a dangerous practice if controls aren't in place to protect data.

Organisations need to implement security processes that identify and inspect hidden data flows. This vital security control protects organisations against data leaks by identifying non-corporate applications.

Mobility
Employees at all levels, as well as third-party contractors, now use portable media, smartphones and mobile apps to access corporate data and applications. This means protecting the traditional network is no longer enough, because the network now extends to any place employees can work (home, hotels, airports, etc.).

Organisations have to put technologies in place to protect the user, the devices and the data, regardless of where the user works.

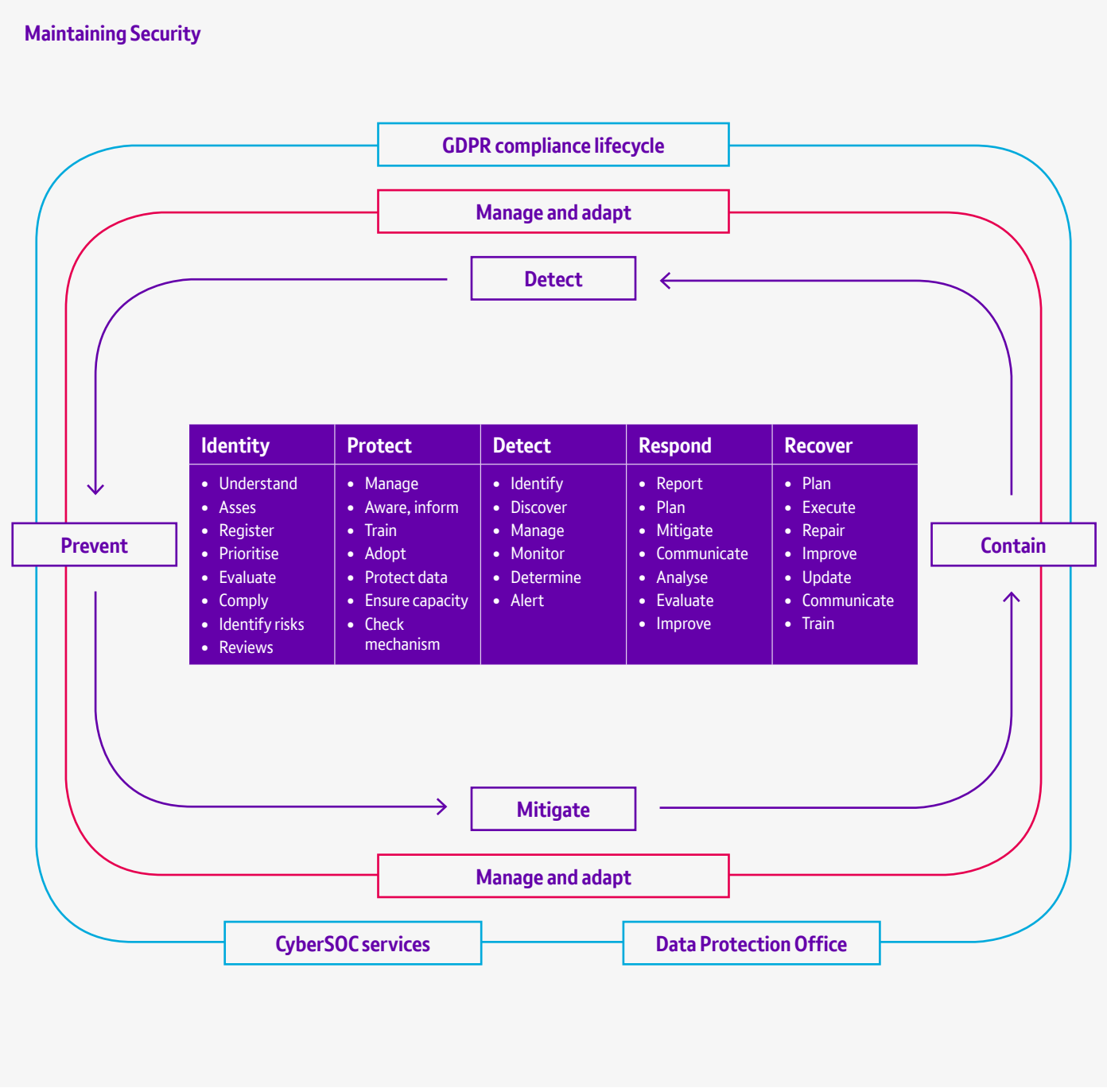
Internet of Things (IoT)
We're in the early days of the IoT, but if an organisation's business roadmap includes the development of new services or processes around this new capability, it has to make data security a mandatory part of the agenda. This is because, with IoT, we will see highly-sensitive information, such as health data produced by wearables, family information in smart homes or geo-localisation by smart cars, shared between devices.

Protecting this data requires expert security consulting services and specific solutions, because the technical foundations of the IoT rely on infrastructure not commonly used in corporate IT.

Managing data security with NIST

To ensure that data's properly protected and complies with the security requirements of worldwide data-protection legislation, organisations have to manage their security systems continuously.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework consists of five stages that organisations can use as a methodology:



Identify
To maintain a secure system, organisations need to review and refresh elements to mirror a continuously-changing business, legal, regulatory and IT environment. The security controls must keep pace with the everyday life of the organisation. Core elements include:

- new data types and changed categories
- changes to the type and impact of the risks related to privacy
- changes to the IT infrastructure or environment
- new software implementations
- the creation of new processes, or changes to current processes
- new roles and responsibilities, and changes to the legal environment
- the appearance of new challenges or risks
- new threats and vulnerabilities.
- To ensure compliance, organisations have to integrate new or changed elements with the current system.

Protect
This stage of the process involves providing and operating the security controls. Organisations have to manage, control and measure the efficiency of the tools and procedures they've implemented, including:

- access and rights management procedures and tools
- security policies, and coordination of these across the organisation
- implemented controls on the infrastructure level
- protection of data-at-rest, data-in-motion and data-in-use
- data-loss prevention, masking or encryption procedures and tools
- data-security awareness training for staff
- inbuilt security control of IT developments
- testing and auditing all controls and procedures.

The operation of security controls requires contribution from the whole organisation. Internal and external IT and security professionals have to work with business departments and the Data Protection Office (legal and compliance) to ensure data, particularly personal data, is appropriately protected.

Detect
The real-time analysis and evaluation of unusual changes in typical daily behaviour can prevent or reduce the impact of security incidents. To improve their security controls, organisations have to investigate and evaluate every event.

This means they need to continuously refresh and review their policies, update their tools, test procedures, evaluate events and improve security controls based on the results. Various technologies are available to manage this. For instance, data-loss prevention tools are able to monitor data, and report or block inappropriate user actions.

Respond
When a security breach occurs, organisations need to be able to respond. And they have to prepare this response in advance — so they can execute communication, reporting and incident management procedure.

When an incident takes place, organisations have to perform these processes with precision and speed, with every relevant person clear about the steps they have to take and when. Organisations must define and plan channels of internal and external communications so they can share information with all relevant parties in good time.

After an event, organisations also have to perform a post-event assessment to identify any further need to improve their security systems, business processes and/or incident management procedures.

Recover
To mitigate the impact of a cyber-security event, and be able to get back to a normal operational level as soon as possible, organisations need to develop and implement suitable recovery plans. This allows them to restore any information or resources affected during the incident. There are a number of important actions to carry out at this stage, including:

- execution of proper recovery planning
- evaluation of previous events and experiences
- improvement of current processes, procedures and configurations based on the results of the evaluation
- training and preparation of employees to handle new challenges
- investigation of opportunities to improve security controls.

Conclusion

In summary, so long as data is protected, digital transformation is the way forward.

The key trends of cloud computing, Big Data and IoT continue to cause major headaches when it comes to data security — but there's nowhere to hide when a breach occurs, and no excuses are acceptable if the breach is a result of security failings such as not implementing appropriate data-protection measures.

When the new EU regulation comes into force in May 2018, we'll see an increase in the level of fines that can be imposed for a data-security breach. But laws and regulations across the world (including within the EU) already enable regulators to impose fines and allow individuals to seek compensation via the courts.

Compliance should involve a holistic review of risk — looking at the classic trio of people, processes and technology. It will also need to be an ongoing effort and not just a one-off review. The new GDPR and the Digital Single Market Directive essentially mandate that security is built-in, not bolted-on as an afterthought, and that data is protected by design and by default.

In a nutshell, security is not just about complying with the rules, it's about protecting your customers, protecting your reputation, and protecting your future.

Authors

Anita Bencsik
Data Security Senior Consultant

Anita Bencsik has been working as a consultant focused on information security for the last five years. She has led and managed major IT and data security projects in sectors such as government, transportation, telecommunication and energy. She has broad experience in aligning business needs and legal compliance requirements to IT security issues. In her current position she is a senior member of the security consultancy team.

Jose Francisco Pereiro Seco
BT Head of Data Security Europe
CISA, CISM, CISSP, CGEIT, CRISC, PCI-DSS QSA, CSSA

Jose F. Pereiro has more than 17 years' experience in the information security and cyber security fields, most of them as a BT and IBM employee. During this time he has held several senior security positions such as Head of Data Security Europe, Head of Security Practice Spain, Security Services Leader, Senior Security Consultant and Security Operations Team Leader. He has worked on national and international projects for top companies, mainly in the banking, telecommunications, government and energy sectors.

He is also a member of the Board of ISMS Forum, Spain, and BT representative at ISF. In his current position he is leading a team to provide end-to-end consulting and technical solutions around the security of confidential records, including intellectual property and other business-critical information. Other highlighted achievements in the past include the launch of the BT Madrid CyberSOC (Cyber Security Operations Center) and building the Anti-DDoS service for BT Spain.

Talk to our experts at:
security.consulting@bt.com

April 2017 | PHME 79409