1

What Is the Process for Achieving State of the Art?

PwC – Gregory Albertyn, Senior Director, and Avi Berliner, Manager

- 'State of the art' is about defending your 'crown jewels'
- Privacy architecture is evolving with new systems
- Cyber governance should be enshrined into company strategy
- Be clear about who is responsible for data sets
- If you're unfamiliar with something, ask the question

As a chief executive, you should fully understand who takes responsibility for guarding the most critical data inside your business.

Your board regularly makes enterprise decisions and choices based on the judgement of these guardians. However, the board simply can't be expected to examine everything in detail, and they need to deploy their time wisely. Yet cybersecurity increasingly requires more of your board's bandwidth because cyber risk continues to evolve in both regulatory and technical complexity: it is ongoing and iterative.

To meet forthcoming EU legislation (for detail see Chapter 2), you are expected to have relevant regard for 'state of the art' cybersecurity. While this might appear a fuzzy description, and it will likely not be defined by EU policymakers, a more solid definition for your own organisation is expected to become clearer as your organisation gains greater insight into the nature, scope and location of the cyber threats you face. However, fundamental to 'state of the art' is a sustained cybersecurity and privacy governance structure, accountable to senior leadership and mandated with continued monitoring of cyber and privacy risk and related enterprise response alignment.

Data privacy and security has traditionally been focused on implementing a set of governance models such as maturing data governance capabilities, performing assessments to create a baseline, and creating a target model to prioritise and manage risks. This has resulted in the introduction of monitoring and reporting tools that are reactive and responsive to threats. Yet, by its nature, 'state of the art' cybersecurity has to be dynamic, identifying and proactively responding in near real time to any new threat.

By its nature, 'state of the art' cybersecurity has to be dynamic, identifying and proactively responding in near real time to any new threat.

Cyber resilient management is about keeping pace with the changing threat landscape, spotting and thwarting threats on the horizon to keep your critical assets and intelligence from falling into the wrong hands. What we are now seeing is the evolution of what is known as 'privacy architecture', a set of guidelines and principles that are embedded into your business and technology processes from the ground upwards, rather than overlaid upon it. This bakes cyber resilience into your operating DNA, with reduced compliance overhead and resource requirements. You should be building cyber and privacy risk governance into your strategic plans as well as your day-to-day activities. 'State of the art' also leverages the exponential capabilities of Big Data. This includes not only the new storage and analytical techniques of constantly improving ecosystems of applications, but also the real-time, batch, and predictive analytical abilities. You will be able to deploy machine learning and other artificial intelligence tools to defend your critical business functions and data from yet unseen attack vectors.

Increasingly, you should adopt 'Privacy by Design' to ensure your security and enterprise architecture incorporates cyber resilience and privacy compliance requirements during initial scoping, and ensure review by all appropriate stakeholders.

To gain comfort on the adequacy of your cyber and privacy compliance programme, you should become familiar—although not necessarily an expert—with professional terms related to 'state of the art', including:

- Encryption
- IAM (Identity and Access Management)
- Anonymisation
- Data masking
- Risk-based activity monitoring controls with appropriate storage and report distribution channels

If you are unfamiliar with these terms, then engage your CISO to explain their importance to operational and regulatory risk.

Furthermore, as a board leader, you should be aware of the risks in:

- the decentralisation of your data, particularly as it is used in the cloud;
- streaming of data—and where the likely attack points might be;
- unstructured data that is not held in safe and protected environments with appropriate controls;
- global data transfer and access to your systems from staff, customers, and stakeholders.

Who should be handling your risk? Many organisations have disjointed threat analysis spread across several functions, physical locations, and systems. To close this gap, you should have a robust, centrally collated threat analysis capability—and an effective, centrally coordinated reactive capability. Based on our experience, the enterprise cyber and data governance capability should comprise a combination of three groups organised to carry out these task and responsibilities.

1. Cyber risk governance committee:

Key members of team: chief information security officer (CISO), chief operating officer (COO), chief risk officer (CRO), head of security, chief privacy officer (CPO), chief data officer (CDO), heads of businesses and functional areas, such as business continuity planning, legal, risk, and regulation.

Main responsibilities include:

- Working with senior leaders to develop cyber risk strategy.
- Classifiying and prioritising information assets—the 'crown jewels'.
- Setting the budget for cyber risk.
- Monitoring the organisation's cyber risk position and reporting on it to senior leaders and the board of directors.
- Reviewing reports from the cyber risk oversight and operations teams and helping prioritise emerging cyber threats.
- Revisiting strategy to adapt the program as the cyber risk landscape evolves.

2. Cyber risk oversight committee:

Key members of the team: information technology team, business support team, compliance/data governance team, and business teams.

Responsibilities include:

- Assessing the active risks the organisation faces, the people behind them, and the assets they threaten.
- Evaluating the effectiveness of the operations team.
- Identifying new threats and improving how information assets are protected.
- Determining how business changes affect the cyber perimeter—including new service offerings, suppliers, vendors, or business partners.
- Monitoring change control and ensuring privacy and security by design for changes to critical systems and data processing activities.
- Overseeing employee training programmes.
- Reviewing new regulatory and compliance requirements.

3. Cyber risk operations team:

Key members of the team: managers and SMEs for networks, information security, fraud, and corporate security. Security operations centre.

Responsibilities include:

- Acting as first line of defence for detecting and responding to cyber events.
- Compiling real-time information from all the groups that monitor cyber threats.
- Producing reports for the cyber risk oversight and governance committees, including number, type, and duration of cyberattacks.
- Maintaining mature "DevOps" framework to provide code and application quality as well as cyber threat scanning and monitoring capabilities.

Adopting this structure can help you attain 'state of the art' cybersecurity, but you should also press your technical people about new, maturing, and expanding capabilities. The cyber and data risk programme should be able to identify your most valuable business assets, know where they are located at any given time, and who has access to them. Your 'crown jewels' are information and processes, which if stolen, compromised, or used inappropriately, could cause significant hardship and damage to your business—and harm your board's reputation for prudence and reliability. Such 'crown jewels' might be trade secrets, market-based strategies, trading algorithms, product designs, new market plans, market or customer data, or other vital business processes. Just as a crown and regalia worn by a sovereign have different values, so too do your own assets. Your executives will become accountable for protecting each of the crown jewels, in the same manner that you expect the finance director to be accountable for your company's financial results. You should be clear who in your organisation is personally responsible for each jewel.

Your governing team, with the right level of knowledge, expertise, and involvement at all levels of the organisation, is required to respond to cyber events. But waiting to prepare your response until after a cyber event is a recipe for disaster. The team should thoroughly understand the risks, the tools at their disposal, and their options in responding before a cyber event occurs.

The development of prepared and tested responses—'playbooks'—is a necessary step in adequately planning and preparing responses to cyber events.

Using the intelligence gathered throughout the playbook development process, each playbook details who should take action, what their responsibilities are, and exactly what they should do. 'State of the art' also means continually revisiting each playbook at appropriate periods, according to classification and risk prioritisation, to ensure updated cyber intelligence gathering techniques, cyber technology, and insurance options. Cyber threats and regulatory mandates remain fluid and dynamic.

If in any doubt, seek advice and consider a 'state of the art' assessment to develop an appropriate road map to help ensure you have the highest level of hardened resilience.

2

The Long Arm of the Law: Understanding EU Legislation's Implications on Cybersecurity

Milbank, Tweed, Hadley & McCloy LLP –
Joel Harrison, Partner

- Two new laws related to cybersecurity in Europe will apply from May 2018—the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR)
- The rules will apply to businesses in EU member states and, in some cases, to non-EU businesses that provide services to customers in the EU
- Firms will face penalties for non-compliance
- Both laws will introduce breach notification requirements. Under GDPR, notification of a personal data breach must be made within 72 hours of becoming aware of the breach

British companies that use or process data must be prepared for European regulations on cybersecurity—or face the penalties.

European Union law related to cybersecurity has undergone a period of unprecedented change in 2016. Two major new pieces of EU legislation—the General Data Protection Regulation[1] (GDPR) and the Network and Information Security Directive[2] (NIS Directive, also known as the Cyber Directive)[3]—will impose security and breach notification obligations on many organisations. GDPR includes penalties, including fines, for non-compliance, and EU member states are required to set out rules on penalties for non-compliance with the NIS Directive. Both laws are set to apply from May 2018.

The UK's vote to leave the European Union has created much uncertainty about the impact of both GDPR and the NIS Directive on UK companies. Given the importance of the UK's having a data protection regime that meets EU adequacy standards, and that the scope of GDPR reaches

beyond EU borders in any case, the requirements of GDPR will most likely apply to many UK companies in one form or another. The impact on the NIS Directive is less clear, although, again, it is unlikely that the UK will abandon its efforts in this area altogether or cease cooperating with its EU partners on combating cybersecurity threats.

General Data Protection Regulation

Scope

GDPR will apply from 25 May 2018. It covers organisations that deal with personal data, broadly defined as any information relating to an identified or identifiable individual.[4] As with the Data Protection Directive[5] that preceded it, GDPR requires organisations to maintain an appropriate level of security for personal data.

GDPR applies to organisations established in an EU member state. It also applies to organisations established outside the EU if they offer goods or services to individuals in the EU, or if they monitor the behaviour of individuals within the EU. So, regardless of Brexit, there are implications for many UK companies that do business with the EU.

Security obligations

GDPR imposes minimum security requirements on both controllers and processors. The direct application of obligations to processors is a significant departure from the current directive, which applies only to controllers.

Under GDPR, controllers and processors must implement technical and organisational measures to ensure a level of security appropriate to the risk that would arise from unauthorised or unlawful processing of personal data. There is a list of examples of what these measures may include, such as encryption and pseudonymisation, and a process for regularly evaluating the security measures. Importantly, the security requirements cover not only the confidentiality of data, but also its integrity and availability.

Where a controller appoints a processor, the contract must require the processor to implement appropriate security measures, even though the processor has its own obligations under GDPR. The controller must also take steps during the term of the contract to ensure that the processor is complying with those requirements.

It is important to note that GDPR does not set a standard of perfection, or establish a regime of strict liability for security incidents. Accordingly, a controller or a processor will not normally be liable for an incident under GDPR if it occurred despite appropriate security measures being in place (as may be the case with a zero-day exploit). So, while GDPR uses the language of a 'personal data breach' to describe a security incident, it does not necessarily follow that any party has actually committed a breach of GDPR.

Notification within 72 hours of breach

Under the new rules, a controller must notify the competent data protection authority of a personal data breach without undue delay and, where feasible, within 72 hours after becoming aware of it. Notification is not required if the breach is unlikely to result in any risk to individuals, but all breaches (whether notifiable or not) must be recorded.

A processor must notify the controller without undue delay once it becomes aware of a personal data breach.

If it is not possible to provide all the required information about a breach at the same time, GDPR allows for the information to be provided in phases, as long as there is no undue delay in providing the information.

If a personal data breach is likely to result in a high risk to individuals, the controller must notify the data subjects without undue delay.[6]

Sanctions for non-compliance

Data protection authorities will have a range of powers for dealing with organisations that fail to comply, as well as giving both affected individuals and representative groups the right to bring claims themselves. Of particular note is the new regime of fines; in the case of a failure to comply with the security or

breach notification obligations, these can be as high as €10 million or 2% of the organisation's total worldwide turnover (whichever is higher). Where a breach reveals a failure to comply with other provisions of GDPR, the fine can be as high as €20 million or 4% of total worldwide turnover.

NIS Directive

Scope

The NIS Directive is a key part of the EU's cybersecurity strategy. It will apply in member states from 10 May 2018. Its scope is more limited than GDPR, in that it applies only to organisations engaged in particular activities; significantly, though, its requirements are not restricted to systems that process personal data. The NIS Directive also establishes mechanisms for co-operation among EU member states on cybersecurity matters, which are outside the scope of this chapter.

The NIS Directive applies to two types of organisations: *operators of essential services* (OESs) and *digital service providers* (DSPs).

(a) Operators of essential services

OESs are organisations—whether public or private—that are of a type listed in Annex II to the directive and that meet certain criteria. Annex II lists operators in seven sectors:

1. Energy—electricity, oil and gas
2. Transport—air, rail, water and road
3. Credit institutions
4. Financial market infrastructure—trading venue operators and central counterparties
5. Health—healthcare settings (including hospitals and private clinics)
6. Drinking water supply and distribution
7. Digital infrastructure—Internet Exchange Points, DNS service providers, and TLD name registries

However, not every operator in these sectors is necessarily an OES. In order to be an OES, an operator must also meet a number of additional criteria, which address the likely overall impact of an incident affecting the operator's network and information systems. By November 2018, each member state must identify each OES with an establishment in its territory.

There is another important exclusion from the scope of the directive: where sector-specific EU law imposes security or notification obligations on OESs that are at least equivalent to the directive, those obligations apply in place of the obligations in the directive.

(b) Digital service providers

The other types of organisations covered by the directive are DSPs. A DSP will be subject to the directive if it is established in an EU member state, or if it offers digital services within the EU. There are three types of DSP:

1. Online marketplaces
2. Online search engines
3. Cloud computing services

Online marketplaces are defined as digital services that allow online sales or service contracts to be concluded with traders, either on the website of the marketplace itself or on a trader's website that uses the marketplace's computing resources. App stores are explicitly included, while pure price-comparison sites are excluded.

While **online search engines** may be self-explanatory, not every service marketed as 'cloud' will necessarily fall within the definition of **'cloud computing services'**. This latter term is defined as a digital service that enables access to a scalable and elastic pool of shareable computing resources; this will include many IaaS services, but may exclude a number of SaaS offerings.

The exclusion for other sector-specific legislation at EU level applies to DSPs as it does to OESs. In addition, DSPs that are micro or small enterprises[7] are not subject to the security and notification obligations in the directive.

Security and notification obligations

Both OESs and DSPs are subject to security and notification obligations under the NIS Directive. While there are some differences between the obligations applicable to the two groups, broadly, both must take appropriate measures to manage the risks to the security of their network and information systems, and to prevent and minimise the impact of security incidents on the network and information systems used to provide essential services or digital services.

Similarly, both OESs and DSPs are required under the directive to notify their Computer Security Incident Response Teams (CSIRTs) or competent authority of security incidents. In the case of an OES, an incident must have a 'significant' impact on the continuity of essential services in order to be reportable, while a DSP is required to report an incident only if it has a 'substantial' impact on its provision of digital services and only once the DSP has access to the information necessary to assess the impact of the incident. The directive does not set out specific timeframes for incident notifications, but merely requires that notification take place 'without undue delay'.

In the case of DSPs, the directive prohibits its member states from imposing security or notification obligations beyond those in the directive itself. (OESs enjoy no such protection.) While this may appear attractive, the requirements of the directive are fairly high-level, so it may be difficult in practice to determine whether a member state is 'gold plating' the directive or merely implementing it. It is also important to bear in mind that the security requirements of GDPR apply alongside the directive, even for DSPs.

Enforcement

The NIS Directive also gives competent authorities enforcement powers over both OESs and DSPs, including the power to impose penalties for non-compliance. The powers in respect of DSPs are intended to apply only in cases where the authority has evidence of non-compliance, whereas the authorities will have the power to investigate *whether* OESs are compliant—although it remains to be seen whether authorities are prepared to play a purely reactive role in practice.

Overlap between GDPR and the NIS Directive

While GDPR and the NIS Directive were adopted around the same time, they are completely separate laws, and their provisions are not always consistent.[8] There are also likely to be circumstances in which an incident triggers notification obligations under *both* GDPR and the NIS Directive.

> While UK businesses would be advised to continue their work on becoming compliant with GDPR, regardless of Brexit, how Brexit will impact the UK's implementation of the NIS Directive remains to be seen.

Take the example of an Irish bank running an application that processes personal data and runs on a cloud computing platform provided by a French service provider. The bank would be an OES and a data controller, while the service provider would be a DSP and a data processor. If the service provider is affected by a security incident that compromises the bank's personal data, the bank would need to notify its data protection authority, its competent authority or CSIRT, and also data subjects if the breach were high risk. The notification to the data protection authority would need to be made within 72 hours, while the others would need to be made without undue delay. This is in addition to any notification obligations under the financial services regulatory regime. Meanwhile, the service provider would need to notify both the bank itself and also its competent authority or CSIRT, in both cases without undue delay.

Time will tell how far these measures will go towards stemming the ever-increasing wave of cybersecurity incidents. Much will also depend on the approach of the relevant

authorities in enforcing these laws, particularly which cases are selected for enforcement action and the penalties that are imposed.

While UK businesses would be advised to continue their work on becoming compliant with GDPR, regardless of Brexit, how Brexit will impact the UK's implementation of the NIS Directive remains to be seen. Given that the UK already is a leader in cybersecurity policy in the EU, it is doubtful that the UK will cease its efforts to improve cybersecurity. In any event, for the UK, cybersecurity is no longer the concern of the technical engineer, but now also the boardroom. Measuring your cyber investments against the GDPR and (possibly) the NIS Directive will take more than a check-the-box exercise. Instead it will require senior leaders to fully understand their business risks and have done their due diligence to ensure their defences are appropriate for the threats their organisations face.

Works Cited

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

3. Regulations are directly effective in the legal systems of EU Member States, while directives must be transposed by the Member States into their domestic laws. As such, regulations are intended to secure a greater level of harmonisation across the EU, while directives often give Member States a degree of flexibility in how their provisions are transposed. Where this chapter refers to an organisation being subject to a requirement under the NIS Directive, this is shorthand for a requirement under the relevant Member State's domestic law implementing the NIS Directive.
4. GDPR maintains the distinction in the current Data Protection Directive between "controllers" and "processors". A controller determines the purposes and means of processing personal data (either by itself, or jointly with others). A processor processes personal data on behalf of a controller. Service providers are often, but not always, processors; the key issue is not how the parties describe themselves in their contract, but the level of discretion exercised by the service provider on how personal data is processed.
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
6. There are three exceptions, although two of them (that the data was rendered unintelligible, such as through encryption, and that the controller has taken measures to ensure that the high risk is unlikely to materialise) essentially mean that the breach is not, in fact, likely to result in a high risk. The third exception is for cases where notifying the data subjects would result in disproportionate effort, but in those cases the controller must still publicise the breach so that data subjects are informed of it.
7. A micro enterprise employs fewer than 10 people and has an annual turnover and/or balance sheet total not exceeding EUR 2 million. A small enterprise employs fewer than 50 people and has an annual turnover and/or balance sheet total not exceeding EUR 10 million.
8. For example, the concept of where a DSP has its 'main establishment', and which authorities therefore have jurisdiction over the DSP, is not exactly the same under GDPR and the NIS Directive. This may lead to confusion in practice.