Clayden | Law

Clayden Law, Prama House 267 Banbury Road, Oxford OX2 7HT
E: info@claydenlaw.co.uk | T: 01865 339640

CYBERSECURITY SERIES: RISK ASSESSMENT AND DATA PRIVACY

It's now clear that (despite the Brexit decision) we are going to implement the General Data Protection Regulation (*GDPR*) in the UK from May the 25th, 2018. The GDPR introduces additional responsibilities onto organisations, to both evaluate any risks to the personal data they hold and then take action based upon such an assessment. Where holding data is considered "*high risk*" a "*Data Protection Impact Assessment"* (*DPIA*) may need to be performed.

Unfortunately, the GDPR does not provide guidance as to a suitable structured risk assessment process. This means it will be for organisations to demonstrate how they judged the risks of holding various personal data.

Don't be fooled into thinking that the decision process will be arbitrary or easy to demonstrate! The GDPR raises potential fines for data breaches (to the higher of 4% of global turnover or €20 million) and, taken together with the new data protection principles of "*accountability*" and "*data protection by design and by default"*, organisations will need to be able to demonstrate how they arrived at any risk assessment decisions.

In terms of cybersecurity, the GDPR introduces mandatory breach reporting for all organisations to the ICO for the first time. Notifying data subjects will depend on the risk of the breach to data subjects' rights.

By May 2018 organisations will need to determine the best way to evaluate data privacy risk to data subjects. Note this is *distinct from risk mitigation*, which deals with reducing pre-identified risks.

In this article, we explore how practical and well-established principles of cybersecurity risk assessment can assist with the assessment of personal data risk in order to comply with the GDPR.

RISK IN THE GDPR

Before exploring risk, we ought to be clear as to what information is within the ***scope*** of any risk assessment under the GDPR. Firstly, it's important to understand the definition of "*personal data*", which goes significantly beyond data that obviously contain personal information (and so beyond the United States concept of personally identifiable information or "*PII*"). Some examples given by the ICO include:

PERSONAL DATA:
"Any information that relates to an identified or identifiable natural person"
Article 4(1) GDPR

- When there is only one employee in a pay band, not publishing that figure, because an individual's salary is personal data.
- If a photojournalist takes a photo of a crowd scene at a public event it is unlikely to hold personal data. If the police take the same photo, with the intention of identifying troublemakers at the event, then the photo becomes personal data – it is linked to people's identities, records their location at a specific time and may influence decisions made about that person.

The GDPR under Article 33(1) states that data breach reporting to the ICO is required "*…unless the personal data breach is unlikely to result in a **risk** to the rights and freedoms of natural persons"*. Data breach notification to data subjects is required under Article 34(1) "*When the personal data breach is likely to result in a **high risk** to the rights and freedoms of natural persons*".

The GDPR thus requires organisations to evaluate risk to personal data **prior** to taking some form of action (see section below for more in-depth analysis on this point under Cybersecurity, Personal Data and Risk Assessment). This may involve evaluating systems and identifying assets/data to protect, choosing suppliers offering sufficient written guarantees, evaluating how sensitive data assets are, considering the harmful impact of any data breach… and more.

DIFFERENT PERCEPTIONS OF RISK

RISK:
"Effect of uncertainty on objectives"
ISO 27000:2016

A big problem with the word *risk* is the variety of definitions used within a single organisation:

- To decide where to invest resources in security, business directors need to identify cybersecurity risks in a comparable way to the other financial, operational or reputational risks their organisations face.

- IT teams discuss cybersecurity risk in a very specific and often more detailed way, where they have knowledge of both a vulnerability in the IT system and a threat that this vulnerability may be exploited.

- Employees may consider cybersecurity risk based on what might happen if they make a mistake, but then balance that with decisions they have to make just to get their job done.

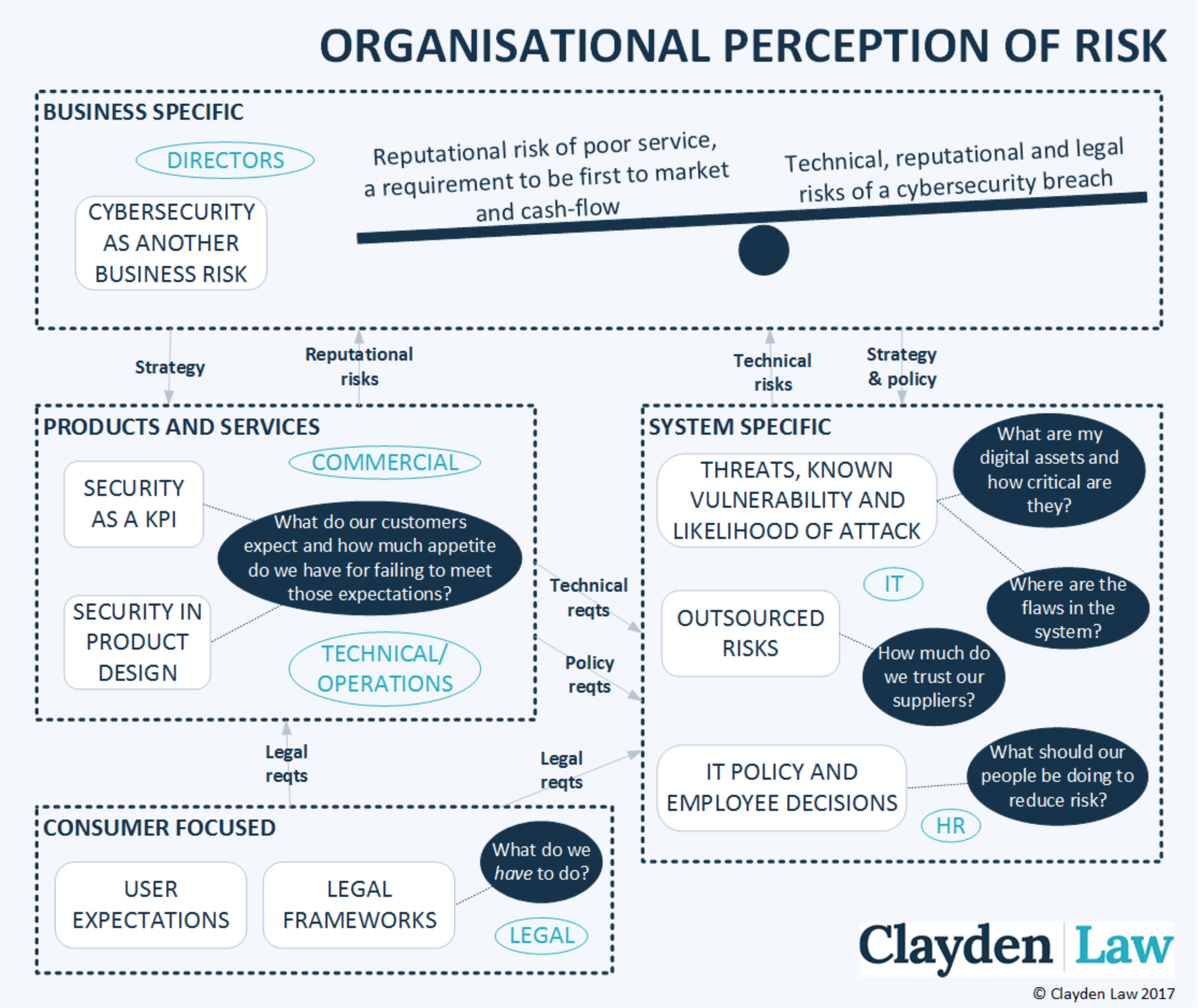
- Commercial teams have to understand how a security breach might affect key performance indicators on their service contracts.

- Product designers and implementers need to assess security risk as part of a product's development and maintenance costs, then balance that against the time constraints of getting a new product to market.

- Legal teams need to understand what an organisation is required to do, based on a number of legal frameworks. The assessment of risk to personal data via cybersecurity breaches is not uniquely a data protection requirement. Legal frameworks in the UK which have developed for cybersecurity, from both a regulatory and common law (duty of care) perspective may expect minimal standards of reasonable care through appropriate risk assessment, perhaps by adhering to a common cyber security standard.

Each function within an organisation has an influence on any justification made for investing in security, however, the different perspectives also complicate the way we discuss cybersecurity before we have even had the opportunity to justify any investment.

The diagram on the following page summarises how all of these definitions of risk interact, how ideally information might flow to decision makers to ensure effective investment and a few key cybersecurity questions that ought to be considered.


ORGANISATIONAL PERCEPTION OF RISK
BUSINESS SPECIFIC
DIRECTORS
CYBERSECURITY AS ANOTHER BUSINESS RISK
Reputational risk of poor service, a requirement to be first to market and cash-flow
Technical, reputational and legal risks of a cybersecurity breach
Strategy
Reputational risks
Technical risks
Strategy & policy
PRODUCTS AND SERVICES
COMMERCIAL
SECURITY AS A KPI
What do our customers expect and how much appetite do we have for failing to meet those expectations?
SECURITY IN PRODUCT DESIGN
TECHNICAL/ OPERATIONS
Technical reqts
Policy reqts
SYSTEM SPECIFIC
THREATS, KNOWN VULNERABILITY AND LIKELIHOOD OF ATTACK
What are my digital assets and how critical are they?
Where are the flaws in the system?
IT
OUTSOURCED RISKS
How much do we trust our suppliers?
IT POLICY AND EMPLOYEE DECISIONS
What should our people be doing to reduce risk?
HR
Legal reqts
Legal reqts
CONSUMER FOCUSED
USER EXPECTATIONS
LEGAL FRAMEWORKS
What do we *have* to do?
LEGAL
Clayden Law

© Clayden Law 2017

CYBERSECURITY, PERSONAL DATA AND RISK ASSESSMENT

The first thing any organisation assessing cybersecurity risk needs to do is manage its expectations since, like any other aspect of an organisation, the aim is to *reduce risk to an acceptable level*. It is extremely difficult to be able to eliminate a cybersecurity risk altogether. Additionally, while the technical responsibility for a risk can be transferred through outsourcing, an organisation retains any associated reputational risk, whether related to breach reporting or performance.

IT systems may have many inherent security flaws but, on their own, this does not guarantee that a serious breach will occur. Often other security layers can compensate to give an organisation the chance to fix problems. Breaches usually occur where there are no further layers

VULNERABILITY:
"Weakness of an asset or control that can be exploited by one or more threats"
ISO 27000:2016

THREAT:
"Potential cause of an unwanted incident, which may result in harm to a system or organization"
ISO 27000:2016

of defence to stop an attacker (implying that investing in a few more layers of security might be a good idea!), or there are a series of existing issues that combine to let an attacker in, normally meaning that applying some attention to detail when choosing/configuring/updating systems would be beneficial.

There are several formal cybersecurity risk assessment processes that can provide organisations an overview of the specific risks they face. These processes allow the various organisational functions to contribute to a decision maker's understanding of risk. Some care needs to be taken when selecting a standard or process as risk assessments may be resource-hungry from a time, management and cost perspective, or produce a volume of material that may not provide a necessary "value-add" to smaller organisations or organisations that do not process data on a large scale.

CONDUCTING A RISK ASSESSMENT

The decision to carry out a risk assessment (including its depth) has conventionally been based on organisational needs. Process-heavy assessments linked to well-recognised standards - such as the ISO 27000 series - may not be suitable for smaller organisations; however, conversely, lightweight versions may lack the necessary credentials for potential customers. Evaluating risk has traditionally been for the benefit of the decision maker, for example, as a prerequisite to be considered for a tender for IT services. Examples of some of the questions raised in a cybersecurity risk assessment can be seen below:

- *What type of IT services (email, websites, backups, hardware etc.) does your organisation use? How damaging would lost control/inaccessibility/breached data be for each one?*

- *How much effort is an attacker likely to put into getting the data? Is there a specific reason (like politics or the value of your assets) that would motivate more skilled attackers to put time and resources into attacking your systems?*

- *What level of ownership do you have? Do you own the hardware? The content? The risk? Where you don't own all three, who are you sharing the security risk with? How much investment will they make in reducing your risk and how much influence do you have over that? How much investment will other risk holders expect you to make in security?*

Privacy risk assessment is a requirement of the GDPR and will be applicable to all organisations from May 2018. This means that companies holding personal data will be expected to carry out a privacy risk assessment, which may include asking the following questions:

1. What is the privacy risk to the information asset (how easily could the confidentiality of the data subject be breached?)
2. What is the risk to the data subject's privacy rights (what impact would a breach have on the subject)?

This aligns with the risk assessment process required by ISO 27001, which states that a risk assessment should include assessing the "*potential consequences*" and "*realistic likelihood*" of a risk materialising. The key difference is that in a cybersecurity risk assessment we are evaluating *risk to the organisation*, in a privacy risk assessment we are evaluating the *risk to its customers* (or other data subjects).

To ensure privacy risk is captured, the cybersecurity risk assessment can be enriched to evaluate privacy risk in a legal context for the purposes of the GDPR. The key is to build-in initial scoping for whether any personal data might be impacted as a result. Therefore, a further question that might be asked is:

- *If a specific vulnerability is exploited (in systems, in software development, via an organisational process, physical security, etc.), might this lead to a breach of personal data? If yes, then personal data is in scope for the risk assessment.*

Risk assessment processes not only *identify* risks, but apply a level of ***severity*** to those risks, so that decision makers can prioritise investment. This involves categorisation into *High, Medium, or Low* (or the equivalent). Where risk assessments in information systems feed into a decision to notify in relation to a breach or in order to inform a DPIA, there will be at least two risk evaluations to be computed to produce an overall *privacy risk rating*:

1. the *privacy sensitivity rating* of the information identified as personal data from the information flows; and
2. likelihood of an event that may impact information security from a confidentiality, integrity or availability perspective.

INFORMATION FLOWS AND ASSETS

Together with the usual consideration of assets in the risk assessment process, to comply with data protection legislation organisations should build in a ***mapping of information flows*** in respect of those assets. This procedure follows the current ICO advice on privacy impact assessments (PIA), (*Conducting privacy impact assessments code of practice*: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf) . Once the information flows have been identified, the risk assessment can be conducted incorporating the privacy risk assessment.

It is worth highlighting that the GDPR departs from the current advice on conducting privacy impact assessments as outlined above. Under current guidance, a PIA ***includes*** a privacy risk assessment procedure based on identified information flows. However, the GDPR requires that privacy risk be assessed ***prior*** to performing a DPIA (Article 35 GDPR) or breach notification (Articles 33 and 34 GDPR). As a result, to avoid running concurrent risk assessment programs it may be worth exploring how any existing organisational risk assessment processes (e.g. via ISO 27001) may be combined for efficiency.

RISK ASSESSMENT AFTER A PERSONAL DATA BREACH

An organisation should steer clear from this approach as it is likely be on the back-foot when it comes to any communications with the ICO. With the GDPR introducing the new data protection principle of *accountability*, this necessitates that risk assessment is conducted **before** an organisation suffers a personal data breach (i.e. an "incident" in IT-speak).

This does not preclude? a company adjusting their risk assessment based on other factors at the time (while of course recording the reasoning for compliance purposes). It is in fact good practice to carry out periodic risk assessments (ISO 27001 goes as far as to require that they be regularly scheduled), to ensure that any changes to the system, or the threat environment it operates in, have been taken into account.

What happens when an organisation has implemented all the security it is within their means to implement, having utilised an appropriate risk assessment to inform it what is most important to protect, and a breach still happens?

If an organisation has complied with its GDPR obligations, including its record-keeping obligations for processing (where applicable), has sufficiently recorded details of its risk assessments, and has complied with its security obligations, the ICO is unlikely to penalise an organisation in such cases even if a breach has occurred.

ROUNDING UP

Risk assessment under the GDPR will apply to all organisations, big or small. While ISO27001 or similar may assist with this process, it may be difficult for some organisations to justify the spend. However, it is essential to utilise aspects of such a standard to ensure compliance under the new law, particularly in relation to cybersecurity breach notifications or conducting DPIAs. The ClaydenLaw team of dedicated privacy and technical professionals can assist you with risk compliance under the GDPR.

Please be aware that these notes have been compiled for general guidance only and should not be considered as specific legal or technical advice.