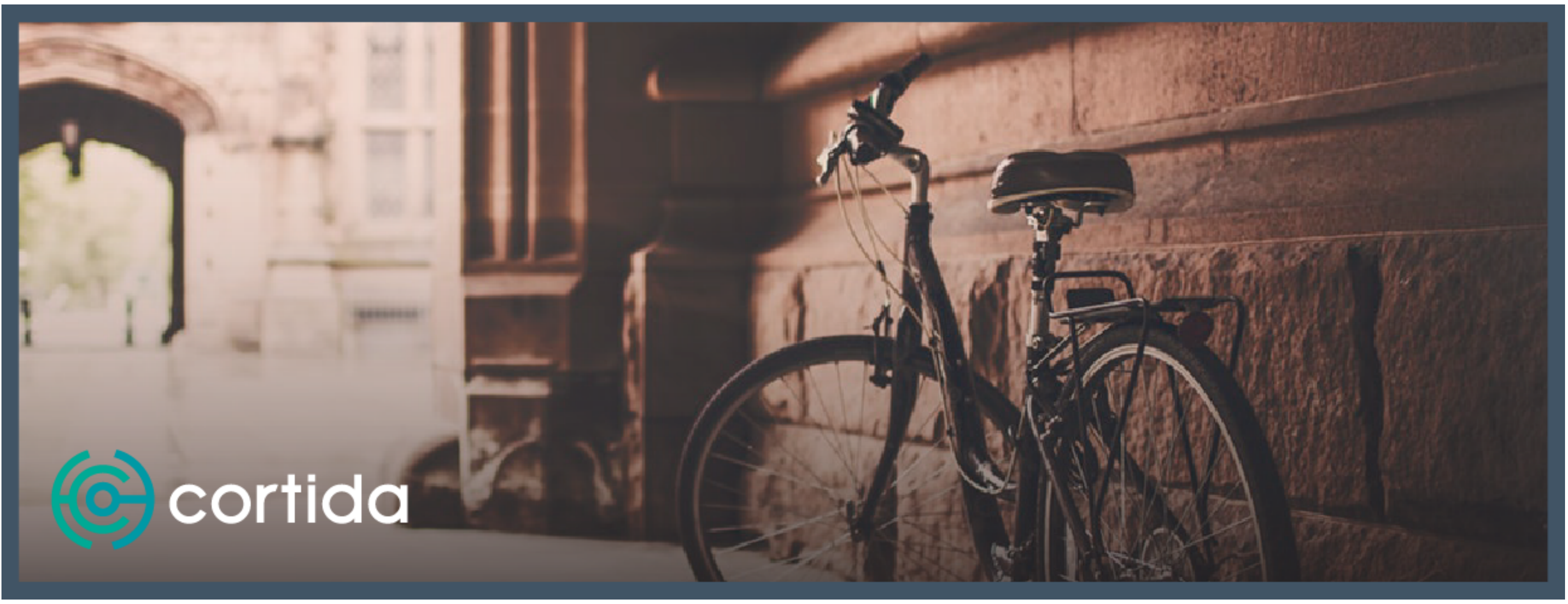

Risk Assessments – Something to believe in

Through good judgement and perhaps contractual or regulatory obligation, organsations are increasingly turning to formal Risk Assessments to understand the risks associated with the data they store, process or transmit. This is a great decision as without understanding the risks it introduces, an organisation is powerless to deal with important questions about how much or little security is required, how quickly it should be introduced and how security spend should be prioritise.

However, with so many potential suppliers of information risk assessments, how do you as a leader identify the right one and dismiss the ones that are simply auditing technical controls – it's simple – look for the small number of suppliers that want to understand your business, its objectives, your attitudes and appetite for risk and how data supports or threatens the objectives and dismiss those simply conduct audits of your security measures. – After all, if a supplier has rushed to assess security measures rather than stopping to think about what is being protected, it's probable you will end up with an over bloated set of measures that will take longer to achieve and will be costlier to implement and maintain compared to one that is more '<u>appropriate</u>'.

When helping oragnsiations understand the notion of 'appropriate' security, I've often used an example of a physical security assessment for my home garage to bring good and bad approaches into focus.

Consider the following scenario:

My garage contains a few spiders and an old bike that was inherited when I moved home. I assume the bike has little value and I'm pretty sure I'm not obligated to protect it. A risk assessment that suggests appropriate security would be the installation of a lock, alarm, CCTV, a moat with alligators and soldiers with crossbows is likely to be quickly dismissed. Moreover, if the security is likely to be unnecessarily difficult and expensive to implement and maintain, the chance of getting me to invest in them is extremely unlikely.

In contrast, a great assessment starts by looking at the bike, recognises it to be an antique penny farthing of considerable value, establishes the exact value and determines whether the risk of loss or damage is above or below my appetite for risk, it then designs a set of security measures based upon an informed analysis. The collation of important facts ensures that as a decision maker I am well informed and have a base against which I can consider any security recommendations. Given the extent of the discovery exercise I am also confident the recommendations are aligned to the value I place on the bike and my appetite for addressing it.

Okay, so a great risk assessment makes recommendations for security measures that are ‘appropriate’ and are in ‘context’ with the risk, however, if the recommendations for addressing the risk are unclear or if they are not weighted according to their urgency – the ability to reduce risk at the fastest rate becomes a more challenging task, so a great partner ensures the recommendations are prioritised in a way that reduces risk at the fastest possible rate. Consider our earlier scenario of the valuable penny farthing in a garage – If the appropriate recommendations are to introduce a lock, an alarm, a CCTV and a moat. A work programme that spends 6 months digging the moat before installing the lock and alarm may result in disappointment.

So in summary, a great information risk assessment provider must be credible to the board and must give you something you can believe in rather than something nebulous, it must leave you a with a great understanding of risk that is expressed in context to your organization and it must leave you certain about what needs to be achieved and with what urgency and priority.

The below list is a quick check list for use when considering your information risk assessment partner.

Does the partners approach include all of the following methods:

- Establishes an understanding of your organisations objectives and attitudes towards risk
- Assesses the organisations data to determine its importance and value and need for protection
- Includes a reasoned assessment of the risk based on probability and likelihood of loss or incident
- Formally identifies an appropriate security benchmark along with any gaps between the in-place measures and the target
- Provides a clear understanding of what needs to be done and with what priority

As borrowed from a previous article, once you know the answer to your risk it becomes easy to make decisions about how to treat the risk and how best to allocate your resources. Once you’ve got the right destination in mind, the job of implementing security and privacy becomes much easier.

Want to understand more about information security and privacy risk? Get in touch at info@cortida.com