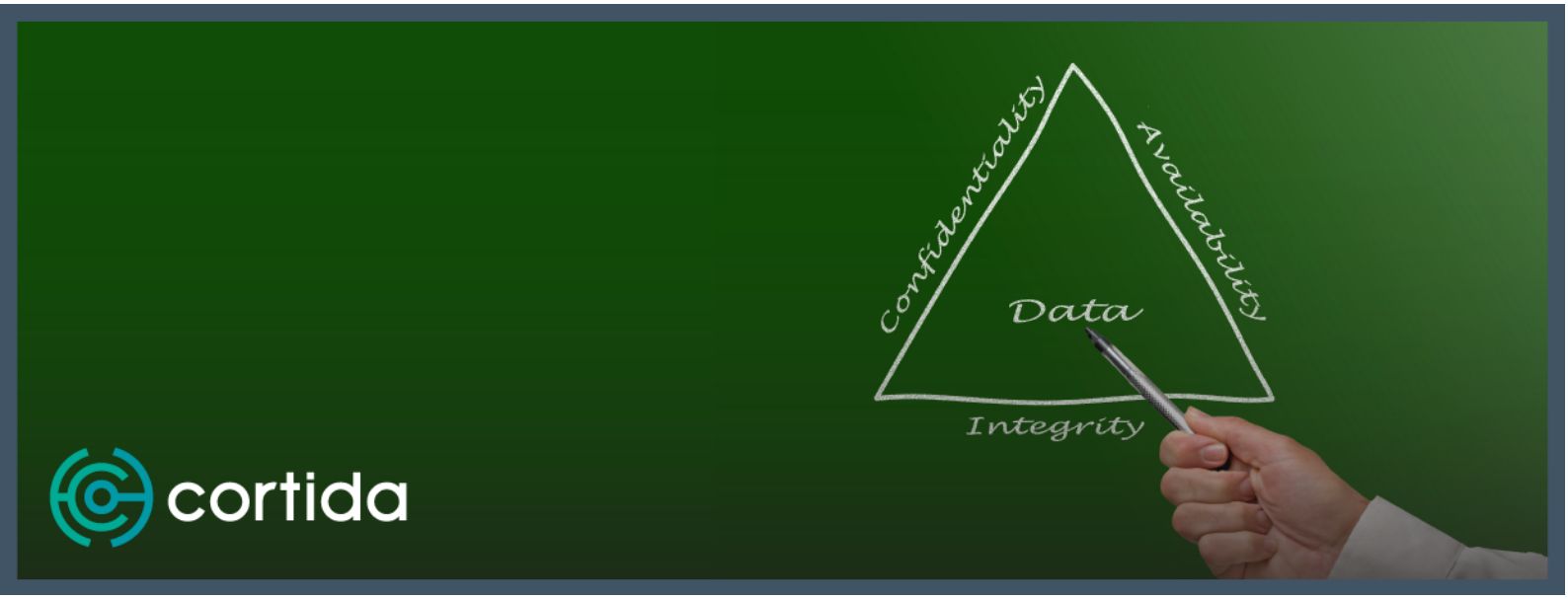


# Data – Be clear on what you are protecting it from

When cyber-attack stories hit the news they invariably talk about exposures of confidential information, however when considering what security measures to deploy, leaders of organisations must think beyond ***confidentiality*** and also consider data ***integrity*** and ***availability***. When combined, these three factors form the CIA triad that can guide organisations through the process of understanding what they are protecting their critical data from.

The intent of C (confidentiality) is immediately obvious as the process for protecting data from theft or unauthorised disclosure. Protecting data integrity is the process of ensuring the accuracy and reliability of the data, and protecting availability is the act of ensuring information can be called upon when needed. In many scenarios, an absence of any one can be very painful however the absence of two or more can be catastrophic – not only is the plane out of coffee, but the landing gear is also faulty.

Organisations often need to adopt all three elements of the triad but to varying degrees of depth. As an example, consider your expectations on a health service provider. As a patient, I want my local hospital to keep personal information about me ***confidential***, and limited to medical professionals who need it to care for me, however I also want it's accuracy or ***integrity*** to be intact and protected from wrongful or malicious alteration so that a I'm not injected with medicines that I'm allergic to or given larger doses of drugs than my body can tolerate. Similarly, If I need an urgent blood transfusion, I want information about my blood type to be ***available*** so my kidneys and lungs don't shut down in a life-threatening way if infused with the wrong type when my record isn't available.

In the above scenario all three are important, however the problems associated with the integrity and availability are likely to have more dire outcomes to my life than a loss of confidentiality. It might therefore make sense that the controls placed around integrity and availability of the data are more rigorous.

However, if I consider my experience as a retail customer, I expect an online retailer to keep my personal and financial information confidential so I don't become a victim of fraud, but once purchased, I might be less concerned about the integrity or the availability of the information. In fact, it might suit me for the data to be wrong or unavailable to potential fraudsters.

In these scenarios, I've taken a view from a personal perspective or that of a data subject. As a leader of an organisation you may also want to consider it from the perspective of your organisations objectives and risks.

For example, as an online retailer you may well be heavily bound by your payment partner to keep payment card data ***confidential*** and you may need to rely on the ***integrity*** and ***availability*** of the payment card record to ensure a charge can be made for a pre-authorised or repeat purchase. This could suggest that security measures should be applied more evenly across these areas.

On a more light-hearted note, imagine if Santa kept your personal information confidential, but exposed the fact you were on the naughty list and the reasons why – no present and public humiliation – sounds like a rotten Christmas. Even worse, imagine that you were meant to be on the good list but it's integrity had been compromised by a maliciously minded attacker or perhaps one of Santa's elves had hit the mulled wine and accidentally edited the wrong list, leaving Santa with a bad reputation.

Once your organisation has successfully identified it's critical data assets, it is worth also considering an assessment of risks and in doing so identifying which elements of the CIA triad are important. Don't forget to consider this from the perspective of the data subjects, your customers and all parties that will have an interest in the data, including your organisation.

Here is a quick checklist of questions that might help you consider your attitude towards the CIA triad.

Thinking about each of the critical data assets processed by the organisation:

- What would your customers' expectations be on the how you apply the CIA triad to each critical data set?
- What do your regulators, or any partner contracts expect in relation to your application of the CIA?
- How would a loss of CIA affect the organisations ability to meet it's longer term objective?
- How would a lack of CIA affect the organisations immediate ability to carry out it's primary activity and for how long?
- Have you positively identified the location of the assets with similar requirements?
- Have you positively identified the security measures required to deliver security based on the importance of CIA?
- Can the assets be grouped together to simplify the application of the agreed security measures?

The answers to these questions will help feed decisions about how much security is required, where and for what purpose and should help you articulate importance to those you make responsible for implementing security. As an additional bonus – it should also help shape and quantify your security spend priorities.

Want to understand more about this subject ? Get in touch at info@cortida.com

+44 (0) 207 164 669
info@cortida.com
www.cortida.com
150 Minories, London, EC3N 1LS