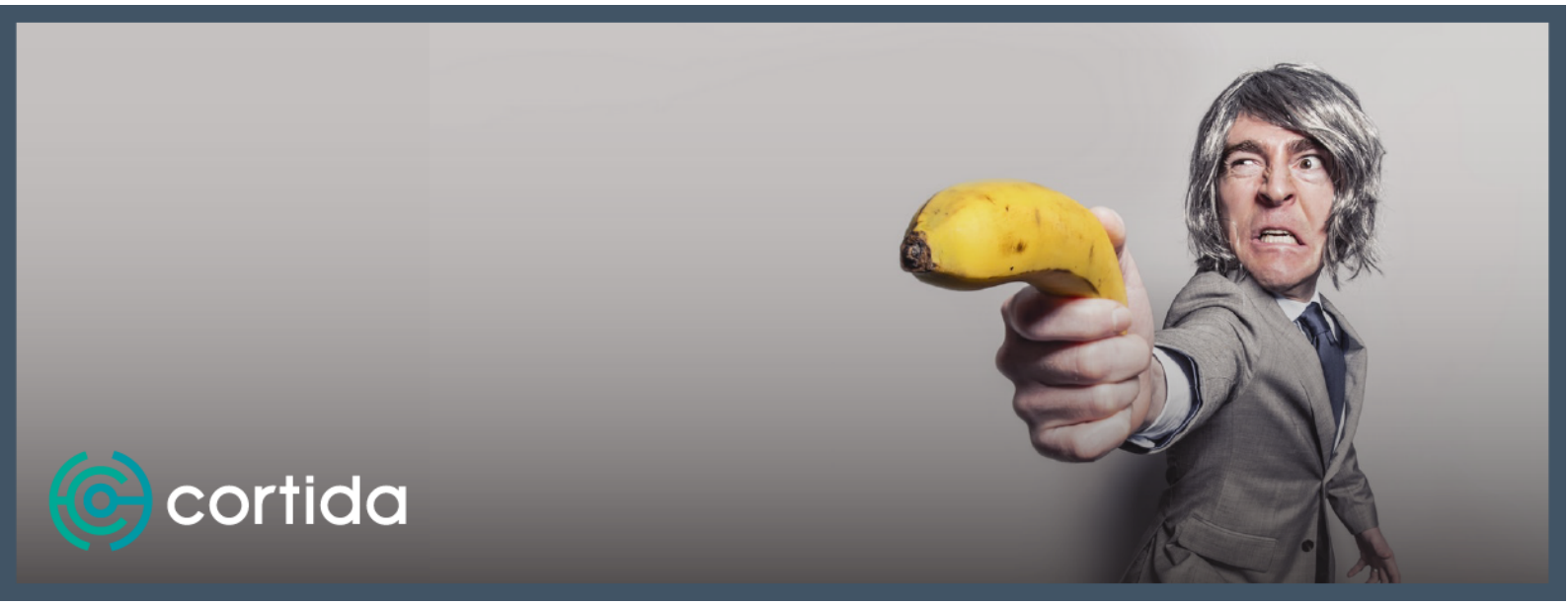

Governance – Save me from the angry mob

In an earlier post *'Information Security & Privacy – It's not my bag baby, or is it?*' I challenged board members to consider how their storage, processing or transmission of data introduced risk to their operational objectives and consider how aware they were of the risks. To build on this, in a later post *'Risk Assessments – Something you can believe in'* I discussed how formal assessments are a way of understanding information risk as well as a great basis for identifying how many or few security measures should be adopted compared to a belt and braces approach, which often results in over bloated security programmes of work.

This combination of factors is a helpful way of knowing where to draw the 'appropriate' security measures line. However, regardless of where it's drawn, organisations often get to the line and then move on to other day to days challenges that call on their time and expertise. The result is often a gradual erosion of security until a week before their next audit when a sprint begins. This is crazy because if you've followed a risk assess and remediate approach, you have a demonstrably good understanding of your risks however when your measures lapse and you need to call on a notion of plausible deniability, you can't – it's shot to pieces. One way to deal with this is of course is not to do the risk assessment in the first place but this is plain bonkers as in the event of an incident there will likely be a queue of people at your desk demanding explanations and 'I didn't know' simply won't wash.

To think about the likely craziness that follows and information or privacy incident, consider who might be in the queue vying for your attention, these could include regulators such as the ICO and FCA, your banking or payment partners, insurers, third party suppliers, employees, shareholders, customers and journalists. A scene from the 1980 movie Airplane comes to mind – the one where an orderly queue of unwelcome guests appears at the side of an anxious passenger, each with their own method of inflicting pain, first a slap or two, then a shake and a slap, followed by boxing gloves, an industrial spanner, a hand gun and a baseball bat – It looks like you've picked the wrong week to give up smoking!

Although 100% security is rarely achievable and in most cases not an appropriate target, there is a way leaders can protect themselves against the gradual erosion of security and privacy standards and diffuse angry blows in the vent of an incident. It is to demonstrate the organisation has adopted a responsible approach to security and can demonstrate good governance has existed. The implementation and maintenance of a governance framework provides an organisations management team and workforce with a set of policies, standards and expectations by which they

must operate, it makes clear the expectations placed upon them and provides a definitive statement about the technical and organisation methods that will be deployed and maintained. For the executive it provides a mechanism by which they are able to assess whether their security objectives are being upheld or require further support, training or investment.

Below is a quick check list that may be useful when considering if your organisation has introduced a form of information and security governance. It is not exhaustive and is not intended to provide the detail of what a security and privacy manager will do on a daily, weekly and monthly basis, this will follow in a later article where security outcomes will be discussed in more detail.

Have you:

- Conducted an information security and privacy risk assessment to identify critical or sensitive data assets that need protecting?
- Identified and documented the people and training required to protect the data assets?
- Identified the documented the processes and technologies required to protect the data assets
- Articulated, documented and distributed your organisations information security and privacy structure, objectives and policies to all employees
- Formed a security and privacy team that will be responsible for introducing and managing the various security aspects?
- Identified and introduced indicators and review processes that will demonstrate how well the security function is performing?
- Embedded a risk process that allows risks above the organisations appetite to work their way through to the executive?
- Embedded a process for assessing how business, partner or regulatory change could impact on your security performance?
- Embedded a process for assessing and managing partners or suppliers that could impact your security objectives?
- Trained all employees on your objectives, policies and requirements?

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

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