Embedding Security – Fingers crossed or part of a plan

I often meet IT teams during their implementation of information security standards, In what feels like Groundhog Day repetition, they are quick to say how the technical controls have greatly improved security and privacy. However, when pressed about what they are protecting and how the management of the information risk has changed or how the technical measures alone will ensure continuous security is obtained, lip biting tends to kick in along with admissions that the management needs more work.

It doesn't take much digging to identify the root cause is that the security project or journey has started in the wrong place and as a result the working practices and management framework haven't been considered and formed.

Starting in the wrong place

Important elements of positive information security typically include the following:

- understanding your information assets and the risks associated with them
- creating and implementing a management framework to oversee and govern the security and privacy function
- defining, implementing, communicating and enforcing policies and procedures to shape secure behaviours
- designing, implementing, managing and testing technical measures to protect data and systems
- designing and implementing systems to ensure technical measures are monitored for indicators of failure, abuse, attack or breach
- being able and ready to respond to and limit the impact of incidents
- raising awareness of security issues and training

When organisations skip the first three items but rush to item four they have often not identified the critical assets that should be protected and there is no basis for establishing whether the measures they are applying are appropriate or where to apply them. An image comes to mind of an empty garage being protected by gold plated security measures while the Mona Lisa hangs in the main dwelling's lounge with the front doors and windows jammed open.

In this scenario, there has been significant financial investment, most likely there was disruption during the implementation phase and the ongoing distraction and cost of managing the security measures. In the case of the Mona Lisa, doing nothing would have saved time, money, effort and would have achieved the same result. Of course, doing nothing is usually bonkers. In contrast, starting you project with a clear understanding of what you will protect will empower you to define appropriate security and privacy measures and also challenge whether the in-place measures are adequate.

Fingers crossed or security by policy?

With the assets identified, it's possible and essential to design and implement a suite of written policies and procedures, these are tools that will direct behaviour and support the organisation as it brings about change. If this stage is missed, the organisation takes a fingers crossed approach to security and hopes it's employees will make good security decisions or that a shiny new piece of kit in the server rack will compensate. In the absence of policies and procedures, staff will quickly believe the organisation's security projects are superficial and may mentally disengage or be clueless about how they can positively contribute – What could possibly go wrong.

As a final point on policies, consider who in the organisation is best placed to oversee the interdiction of new policies. Of course IT professionals will often have a superior technical understanding of the issues compared to the board, however when it comes to driving change through policy, process and management – is the board better situated for this?

Hoping or checking?

Beyond understanding the information assets and creating policies, a successful implementation of a security or privacy standard must include the formation of a management framework that ensures a mechanism exists for formally monitoring, measuring, analysing and evaluating the chosen protections. Without such a mechanism and given that the introduction of standards is a gradual process over a number of months, the absence of the framework will constrain the introduction as well as its long-term success.

How does your organisation measure up on a management framework, here is a quick checklist to help you consider this.

Have you:

- Identified key people, critical roles and responsibilities for managing and maintaining security and privacy?
- Identified and documented the people, process and technology measures required to maintain security and privacy and recurring activities and frequency required?
- Established a mechanism for evaluating the extent to which employees are security and privacy aware?
- Identified the indicators and audits that will establish whether essential activities are being conducted?
- Established a mechanism for documenting and progressing problems and shortfalls?
- Established a mechanism for determining whether the security measures you have in place continue to be appropriate?
- Put in place a mechanism that identifies incidents and reviews how the organisation has responded to them?
- Introduced a mechanism for assessing how privacy and security will be impacted by planned change?

An absence of just a few of these factors can quickly bring most programmes to a halt or embedded arrangements into disrepair. If the policy framework is a definitive statement about how the organisation will achieve security and privacy, the management framework is the check by which the organisation ensures it will maintain appropriate and relevant security.

If you currently have a stalling security standards project or are about to initiate a new project, consider your starting place carefully and, if required, seek professional help to get the project back on track and the greatest chance of success from the outset.

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