Image: ThinkStock/78742692

MORE CONTROL, LESS RISK

When it comes to dealing with cyber security, technologists must focus more on threats and controls and less on risk, says Neil Cordell.

doi:10.1093/itnow/bwv039 ©2015 The British Computer Society

To ensure that an organisation is properly protected in today's connected world, it is critical to focus on the real threats to that organisation's assets and the controls that need to be in place to protect these assets against the threats.

Risk comes from the deficiencies in the implementation of the controls that should be in place to protect these assets against the actual threats. A proper evaluation of risk can only be based on a true understanding of the threats, assets and controls.

Last year's report, 'Risk and Responsibility in a Hyperconnected World' - published by the World Economic Forum in collaboration with McKinsey & Co., offers an interesting element of insight into the true mindset of some of the technology industry's economic actors when it comes to cyber security and controls.

Controls and productivity

The data in the report suggests that 88 per cent of all respondents saw controls related to cyber security as having zero or only a moderate impact on front-line productivity. However, the authors of the report decided to interpret this result by stating that 'cyber resilience controls are having a significant impact on front-line productivity'. It is hard to understand how such a conclusion could be reached, raising further questions around the authority of the report and the agenda of its authors. It seems to only take into account the view of the technology industry respondents – 50 per cent of whom believed that these controls are a 'major pain point for their users' and a factor that 'limits the ability of [their] people to collaborate'.

The difference of appreciation on this matter between technology and non-technology respondents, which, although reported correctly, is not explained in the report - is one of the shocking facts of the survey. A discrepancy on such a scale could suggest a serious disconnect between the technologists and the business users.

Technologists versus business users

A number of factors can contribute to the differing perceptions of the impact of controls on productivity. The report was derived from interviews with industry leaders, a cyber risk maturity survey and the subsequent analysis of these responses. In contrast, our observations, analysis and conclusions are based on over 20 years of real life field experience working in various roles for end user businesses.

In our experience, technologists are making decisions on what controls to implement based on their own expectations of the impact they will have on either their own or the business's productivity. In doing this, the technologists are taking a very cautious position - avoiding anything to adversely impact the end users, rather than putting in controls to actually protect the business. This stance is often taken because of criticism from influential or vocal users in the past.

Business users are assuming that the appropriate controls are in place that have not actually been implemented. Therefore, these users have the perception that the controls have little or no significant impact on their productivity, because many of these controls are simply not in place.

Business users are assuming that the appropriate controls are in place that have not actually been implemented.

Whilst the different perspectives of the technologists and business users described above are at the extremes of the problem, our experience is that, in reality, these positions do exist to some extent in most organisations. Consequently, there is a fundamental misunderstanding between the technologists and business users which leads to many organisations having a false sense of protection against cyber threats and cyber-crime.

Remove this disconnect

The first action that technologists can take is to engage in a positive dialogue with the business users about controls. This step is more complex than it may initially appear, which may explain why it doesn't happen as often as you would expect for a variety of reasons.

The most common reason is that many technologists are unable to communicate the situation in terms and language that the business users can understand. In turn, the business users believe that it is just a technology problem in which they do not need to be involved.

However, there is no silver bullet and the answer to narrowing the gap will always rely on associating people, process and technology, usually defined in that order, when talking to the business.

The way to initiate a meaningful dialogue between the business and technologists around controls is to focus on the real threats that the business is facing. It is also necessary to jointly identify with all key stakeholders the key information assets and business processes that the threats may target. It is important to realise that this will vary depending on how a particular business operates and its reliance on technology to execute business.

For example, an e-commerce retailer is completely reliant on its website to transact business - so the highest priority threats will be cyber-attacks directed at its website. On the other hand, a catering company providing outsourced services to large corporates is much more dependent on its supply chain and payment systems - so its highest priority threats will relate to these systems and not its website.

Once all the stakeholders have agreed on the real threats to their specific business, these threats can be ordered by their relative importance to obtain a shortlist of the highest priority threats to focus on. For each on the highest priority threats, the most appropriate controls, which may be people, process or technology oriented – to protect from that particular threat can be determined, discussed and agreed amongst the stakeholders.

The objective is to create a meaningful set of important controls, which will provide a high level of protection against the threats and can easily be measured on a regular basis.

When you have an objective and measurable way of determining how effectively the key controls have been implemented to protect the key information assets, it is then possible to prioritise the improvements in these key controls to better protect the organisation against the actual threats that it is facing.

This forms a threats and controls framework, which allows management to make informed decisions on how the limited available resources (budget and time) can be used most efficiently and effectively. Only through this understanding of the threats, assets and controls, can a proper evaluation of risk be made.

Where to focus to improve cyber security

Technologists should focus on having a meaningful and open dialogue with their business users and all other stakeholders focused around the real threats to the business and the necessary controls required to protect the business assets from these threats.

It is key to remember that there is no magical software and hardware solution, because all solutions will involve people, process and technology.

The creation of a cyber security strategic roadmap derived from a threats and controls framework is key to helping the stakeholders develop a real understanding of the way their business is protected and the level of future investment in cyber security that is required to maintain or improve the desired level of protection.

www.bcs.org/security