All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Enough with the technical stuff already

Technical security is all fine and good. Even better when there is a theoretical basis for it and experimental evidence confirming its basis and measuring its effect. But the problem we all face is not technology or the lack of it. The problem we face is now predominantly operational, and more specifically, making and properly executing reasonable and prudent decisions regarding protection programs.

Making reasonable and prudent protection program decisions

Making reasonable and prudent decisions requires an understanding by someone involved in the process of what is and is not reasonable and prudent. Of course you could make good guesses a few times here and there, but because there are something like a hundred such decisions that most companies should probably make, and many of them involve five or more alternatives. Even if you guessed right 90% of the time about the different alternatives, which is statistically almost impossible, that would leave you with perhaps 50 wrong decisions.

So you need to have people that understand how to make good decisions, and you need to do it in the specific context of the business. The reason the context is important is that all of the alternatives are reasonable and prudent under some circumstances. Otherwise, they would be dismissed as alternatives out of hand, and we would bother to consider them at all.

Reasonably and prudently executing on those decisions.

Of course even if you make good decisions, you need to carry them out in order for them to be effective. Thus the notion of plan, do, check, act of the ISO27000 series. This is the management feedback system that allows effective control over a protection program. These days, there is a lot of automation in the form of workflow systems to help get this right. This reduces mistakes and makes the whole process more effective, although sometimes we question the efficiency of it in small operations.

At the end of the day, however, even the best workflow system cannot cause the implementations to go right every time. When the management decisions is to have a quarterly review of high-consequence systems and their operations, the review only takes place when the systems are properly classified as high consequence. The method for determining consequence should normally consider interdependencies, and in many cases, the testing process to verify that the dependency analysis is correct fails to undertake to systematically disable all of the things that are not dependencies to verify that they are not in fact dependencies. The cascading effects are tricky and we often miss them and the systems and methods in place today don't adequately address them. Which is the point of this article.

Conclusion

Technology to support the vital non-technical aspects of protection is often poorly done. Most of the spend and effort appears to be going to chase down the ever-lingering flaws in technical implementation. But the reason those flaws are hurting is often because of poor or poorly executed decisions. We need more focus and funding for better decisions and support.

