Be A Conscientious Risk Manager

Stephen Nardone, CISSP
Director, Security Practice
Technology Solutions Group
Connection

WHETHER YOU ARE A CIO OR CISO IN THE FEDERAL, STATE OR Local, Education, or Commercial Business areas, you are all faced with same challenge, whether you accept it or not.

In the security risk management world, if the malicious actor wants into your network, they will figure out a way to get in. You of course still need to build a comprehensive risk governance and management plan, but that plan must be built on the premise of how you will respond, when the breach occurs.

> "Create a strategy whereby you frequently identify the threat, and measure the risk against that threat in your as-built infrastructure. Test frequently, outside and inside, using he same tools and techniques the malicious actors use."

Having spent 38 years in Information Security, the one constant that I see, is that the individuals who make it their business to steal or disrupt your data, are better funded, better trained, and have unlimited hours to execute their trade. What we hope to achieve is being a half-step behind at them worst case. There is no way to stay in step, and a step ahead is out of the question.

So what does this really mean to the conscientious risk manager. Create a strategy whereby you frequently identify the threat, and measure the risk against that threat in your as-built infrastructure. Test frequently, outside and inside, using he same tools and techniques the malicious actors use. Test user security awareness, as we know it only takes one click of a phishing email malicious link, to potentially bring down and entire enterprise. Measure, document, prioritize, and build a risk roadmap strategy to keep risk mitigation focus on those most critical exploitable areas.

Three Top Security Imperatives

Keep in mind that your top three security imperatives are: Reducing your threat exposure, enhancing your response and recovery times, and increasing security visibility. What does security visibility mean, implementing the people, process, and technology in key security areas, to give you a fighting chance to detect, and react to malicious and advanced persistent threats.

Let's talk people, process, and technology. We all know users are the weakest link in any security chain. Not because they have sinister intent, although sometimes they do, but primarily because in todays high-powered technical, mobile, and social world, it is commonplace for a lapse in judgment to occur. We live in a rapid–fire, high-availability, high-output world, and mistakes can and will be made. So make is less commonplace, train and educate often, and monitor closely for when that lapse in judgment occurs.

Process: Again our high-powered technical, mobile, and social world often demands we run at warp speed. Who has time to document? Well — make the time. Good documentation to include process, policies and standards, as well as a documented and managed configuration control process, will help keep you more secure. Every process, policy and standard document has to have an assigned owner, has to have a designated review date, and has to have an oversight or governance process. All roles and responsibilities need to

be included in the documentation, and the expected outcome needs to be defined. Make the time to prepare and socialize your critical information security program documentation.

Technology: Many risk owners fall prey to purchasing every piece of security technology available, at what I like to call the security "choke points", end-point, network, edge, gateway, etc. This is just what everyone does. However, why not use the process we discussed above - measure, document, prioritize, and build a risk roadmap strategy - as your guideline for what you purchase and deploy for technology. Ask yourself - what is so wrong with selecting and implementing a product, only after you validate how it will help you manage your documented security risk? Of course the answer to that is — nothing.

Focus on Seamless Collaboration

You have documented your risk, you have prioritized your risk roadmap, and as a result you know the very specific technology, or set of technologies, you need to implement first. Most importantly, your technology selections should focus on products that collaborate in a seamless way. In other words, your end-point, edge, network, gateway, sandbox, etc., security technologies all talk to each other. We call this approach to complete security visibility across the whole landscape, Unified Security Stack. And, don't forget that all technology must have a people and process component as well.

Good information security risk management and risk governance does not come by accident. It takes planning and execution. In the end, although you may not keep the bad guy out, you will be better prepared for when. ■