STRATEGY, RISK-BASED FRAMEWORK KEY TO CYBERSECURITY

Steve Struthers
VP of Security Services
DynTek

Historically, IT teams have taken a reactive approach to cybersecurity much like they have with all of IT: reacting to user complaints and network problems and purchasing products in an adhoc fashion to — hopefully- fix the problems.

"But security doesn't work that way," says Steve Struthers, DynTek Vice President of Security Services. "Security demands a completely different approach, one in which you are defending against the unknown."

In the above scenario, IT often spends a large portion of its budget on a big-ticket item based on fixing the single event, and runs into problems when the team asks for additional funds to address other issues that are also important.

Increasingly, however, companies are taking a different approach to security, one that involves creating a security strategy based upon the company's risk profile and mapped to the NIST security framework. Having a strategy in place, knowledge of business risk, not just IT risk, and clearly communicating where security gaps are in relation to NIST security controls make it easier for Chief Security Officers to win budget for cybersecurity spending, says Struthers.

DynTek's Security Team, along with Shaun Land, DynTek's Principal Architect for Security Strategy, has created a simple, one-page template, that easily shows customers a set of technical controls, derived from NIST and similar frameworks, and maps out which products from various vendors can be applied to address those controls.

THE SECRET TO EFFORTLESSLY GROWING YOUR IT SECURITY BUDGET EXPONENTIALLY.

The template, which Land originally developed when he was a client of DynTek, allows customers to see what areas they have covered and where their security lapses reside. Other vendors trying to represent security architectures in graphic form, often ignore standard frameworks such as NIST, and deliver documents that "are so complex that they look like Intel chip designs" said Land. "We then help CSOs build a plan that addresses which gaps they want to fix first, which risks they want to accept and cover, and help them build a strategy around security," says Struthers. The end result is a 1-to-3-year strategic security roadmap based upon the company's risk profile and appetite.

The NIST Framework, a 40 page document which breaks down security concerns into Functions, Categories, and Subcategories, and provides a way to organize, conduct, plan security goals and drive improvements for small to large enterprises and across different industries. It does not, however, include a specific risk management process or specify any priority of action, instead leaving that up to individual organizations based upon their own risk profiles.

Since business risk management may be a little out of the comfort zone for technology focused directors and CIOs, DynTek has tapped Land's expertise in risk management and strategic decision making, giving the company and its clients a strategic advantage. "We simplify the task of translating NIST to controls, and we help IT understand what it means to be in the recommendation business, relative to security" says Struthers.

DYNTEK
DYNAMIC TECHNOLOGY SOLUTIONS

Shaun Land
Principal Architect for Security Strategy
DynTek

> **WE HELP CHIEF SECURITY OFFICERS ORGANIZE, COMMUNICATE AND BE SUCCESSFUL IN THEIR PROGRAMS.**
>
> **SHAUN LAND**

DynTek also helps IT understand that the business executives and the board should be the ones in the 'decision business.' Rather than telling business what IT needs to buy, DynTek teaches IT how to speak with business leaders. "We help IT explain what the risks are and how they impact the business in a quantitative basis, showing that they have estimated the cost to the business if they don't take action, and the cost to remediate as well" Land said.

Helping IT better communicate in this way casts them in a better light, since at many companies, IT and business are at odds, he said. "The change in processes and communication helps ensure the success of the overall program. As a result, they can now communicate clearly with the business, which gives the IT and security team a better chance to get the budget and resources they need to be successful."

DynTek also helps customers develop their full policies library and primary procedures library. As Land describes it, "We move them from "there's too much to do", and "where do I start?" – a state that never goes anywhere – to literally within a few weeks having security policies ready for full review by the business, no matter what industry they are in. "We help CSOs organize, communicate and be successful in their programs."

FRAMEWORK FOR SECURING CRITICAL INFRASTRUCTURE CYBERSECURITY

CREATED BY THE FEDERAL NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY RESEARCH (NIST)

The federal National Institute of Standards and Technology Research was created in February 2014 to provide security guidelines to reduce federal agencies cyber risks. It has since become a major part of the national conversation about cybersecurity.