Using Test Sites to Decrease Incidents and Increase Buy-In

One of the many difficult tasks in security leadership is showing senior management and other business leaders exactly how, where, and how much security investments positively impact the bottom line (assuming, that is, that security's impact is positive).

By Marleah Blades

Data for metrics should be readily available in a well-managed security function, but is it always persuasive? The impacts of security-related events and decisions are often complex, making causality difficult to define. That is, the security leader may see that a sales increase corresponds with a certain risk mitigation decision, but it may be hard to show how that decision – and not the recent marketing campaign, or the upcoming holiday weekend, or the drop in oil prices – definitively caused the increase.

In the most recent session of the Security Executive Council's Next Generation Security Leader Development Program, Francis D'Addario shared a proven tactic he has used in multiple organizations to tackle this problem: testing security investments in pilot locations. D'Addario has led security and risk functions for Starbucks Coffee, Hardees Food Systems and The Southland Corporation (7-Eleven). Each of these companies introduced risk mitigation changes by first implementing them in a series of test stores. A cross-functional team would identify "control" stores – locations in similar neighborhoods with similar sales figures and client demographics – and compare results across tests and controls over a defined period of time.

When the method was employed to decrease robbery incidents in certain 7-Eleven stores, the company realized a nearly 90-percent decrease in incidents and overall risk improvements estimated at $98 million – in only three years.

According to D'Addario, the pilot/control method allows the security leader to promote confidence in security's ability to influence outcomes, because it provides persuasive or even conclusive evidence of causality. It can also make it easier for management to buy into a solution.

When you're proposing a technology-based solution to a particular problem, for instance, "the buy-in requirement is not to present the final cost of adoption and deployment," he says. That approach may lead management to focus on even a trial solution as a long-term cost rather than a net benefit. "The requirement instead is to implement a free or at-cost innovation (product providers will often allow for trials on these terms), in a place that really needs it," D'Addario continues. The up-front cost here is minimal, so buy-in for the first trial phase is unlikely to be a great challenge. If ongoing metrics show the solution effective and valuable, they will automatically provide persuasive evidence of value upon which you can base a proposal for an expanded trial or a roll-out.

Tests like these work best when security is thoughtful and careful in selecting sites and informing peers, says D'Addario. "If you're looking for a robbery remedy or or policy violation remedy, you want to look to incident reporting data to find the places – buildings, stores, departments – with the highest rate of incidents. Then you want to do three things. First, inform your audience you're going after the issue. Then bring in cross-functional partners by finding out the intricacies of how their business operates and what metrics they already use. And have the business operators or marketers – people familiar with selecting controls for test groups – help you select your controls." These three action items will make the testing process more accurate and meaningful and will also create allies across the organization.

Multi-location businesses are not the only types of organizations that can benefit from this process. The test/control method is just as useful when scaled down or when applied to a problem within a business unit or a single location. D'Addario shared another example in which his team decided to implement an IT tool that would alert them when employees visited unauthorized websites. As their control, they ran the tool in the open. "We wanted to see what the activity was before we applied it," he says. "We took the existing acceptable use policy and re-communicated it to everyone on the network. We let everyone know we had a tool that could identify if they were visiting such sites and that we would adopt a three-strikes policy in the pilot offering. We measured how many hours people were spending on unauthorized sites as we were bringing in the accountability elements of the policy. As we started citing people for infractions, we were able to demonstrate millions of dollars of unauthorized network time usage going away on our network. Just by taking an approach within a known environment and being conspicuous and transparent, we not only saved productive HR time, but we saw that we didn't need as many servers as we thought we would the next year, because the activity had a net effect on server requests."

Measuring indirect impacts is often critical to defining the true total value of a solution, and the test/control method makes it easier to show how risk decisions bring unexpected results. It's clearly persuasive to management when you are able to report that an application is profitable in month one, but if you can include in that equation the reputational impact of the customer care your changes have shown, increases in service scores, higher productivity and other such effects, management will wonder how they could possibly say no. SECURITY

About the Author:

Marleah Blades is senior editor for the Security Executive Council, a leading problem-solving research and services organization focused on helping businesses effectively manage and mitigate risk. To learn more, e-mail contact@secleader.com or visit https://www.securityexecutivecouncil.com/sm. You can also follow the Council on Facebook and Twitter.