SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Leadership > Executive Communication >

The Biggest Gap in Security Success: Not Getting Executive Agreement on "Why?"

By Bob Hayes and Kathleen Kotwica

One of the recommendations we frequently make to new and struggling security leaders is to always be prepared to answer the big four “executive questions”. Budgets, projects, new positions, expansion of headcount, new technology, elevated role, or even travel evoke the inevitable: Why, what, how, and how much. This may seem simplistic, but it can get to the root of all types of program limitations, vulnerabilities, inefficiencies, lack of executive influence and even failures.

Of these questions seldom addressed in advance, the one most frequently assumed or skipped over by many security leaders is “Why?”. Yet it’s the most important question to win support. Friedrich Wilhelm Nietzsche was a German philosopher born in 1844 and influenced the discipline. One of his most famous quotes is: “People will do almost any “what”, if you give them a good “why”.

Agreement on “why” is the first step in translating your strategy into a compelling leadership message. Most executives have little firsthand security experience. Despite executives owning the risks you are trying to mitigate and having the authority to accept or mitigate the risk, they seldom have any depth in understanding the risk severity or consequences. The most critical first step is to get their agreement on “why” we need to take mitigation measures.

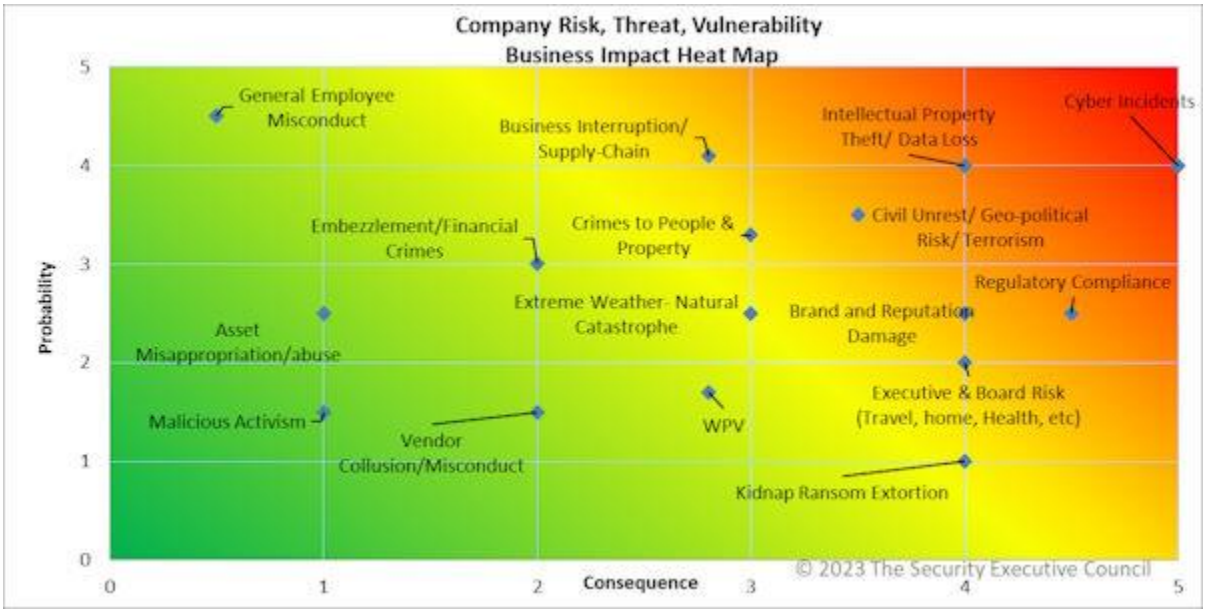
The Sticking Point: Why?

"Why are we doing this?"

This question, unfortunately, is sometimes asked by senior management before security leaders have answered it for themselves. Why does the business need these security programs? Why should I care? Why should we spend this much money on this? Why do employees have to do awareness training? Why require security duties of site managers? Why do we need a GSOC? Why does security have to travel with the executives? Why are business unit leaders being asked to commit their time to security tabletop exercises? Why should we approve this capital project? Why should I take this to my boss for approval?

The answer to "Why?" should always point to a specific, organization-level risk. No action or decision should be undertaken by security unless it can be connected directly to a specific risk to the organization. Absent this connection, any security expenditure, proposal, program, or service will represent a waste of organizational resources.

Using a risk heat map is a great way to visually articulate the why.



Everything security leaders do should revolve around risk mitigation – so why is this so often the hardest question of all?

Sometimes, it's because security programs are launched based on a demand from senior management, motivated by, for instance, an uptick of a certain type of event in the news cycle. These "issue of the moment" programs may not be attached to specific risks to the company at all.

Sometimes it's because the security function is tied to doing things the way they have been done in the past. Particularly if the security leader has been hired into a legacy department, or if the governance structure is such that the leader has little control over higher-level decisions, asking why certain programs exist may not feel intuitive. This leader may not feel they have the authority to ask such questions, and they quite likely don't feel they have the time.

What and How: The Low-hanging Fruit

These tend to be the easiest and first questions for security leaders to address when making a proposal or introducing a program. Too often security leaders, to their detriment, focus exclusively on these two. They never or too late address the why in terms the executives understand.

1. **What** is our security vision, mission, strategy? What are the relevant programs and services that make up the security function. What technology will be deployed? What resources will be impacted? What regions will this entail? What disruptions will this cause?

2. **How** will you do this? Vendors, contractors, or matrixed organization? How will security deliver its services and programs – through a centralized, distributed, or governance and oversight model? How will this impact the risk or issue? How long will it take to see the results? How many other functions will be impacted? How much inconvenience will this cause? How will the complicate the existing process?

These are important and expected answers you must present or be ready to address. Way too often in our careers we seek innovations and new services that can be deployed. We are often drawn to the new shiny objects. Unfortunately, we often overlook their relationship with why.

[For more on service delivery models, read *When Your Security Proposals Keep Hitting a Wall, Try Looking at Your Security Service Delivery Model*]

How Much: Easier with Metrics

Many security leaders can quickly and accurately answer the easiest "how much" questions. How much will this cost? How much of the staff/employee's time will it require? How much will this add to their existing workload. How much time does it take to set up? How much bandwidth will these new technologies require? How much money do we need to invest in this? How many business units need to be involved? How much business interruption will result from the implementation or maintenance of these services and technologies?

All of these are must haves when making the proposal. But do not forget that sooner or later you will have to answer other more difficult how much questions. How much impact will this

have? How will you measure the risk reduction? How much value did this investment add versus the cost? How much safer are we? How much less likely are we to have this problem because of this investment?

Having a solid metrics program helps exponentially with questions like these and then goes beyond counting to providing meaningful insight into the function and its performance.

[For more on security metrics, visit Security Executive Council's Insights on Security Metrics]

[For more on understanding security's stakeholders, read ***Three Ways to Improve Buy-In from Your Internal Customers***]

The Security Executive Council can help build the success story for your security function. Let us help you develop the most valuable answers to why. Contact us to find out how.

Visit the Security Executive Council web site to view more resources in the Security Leadership : Executive Communication series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

