Planning for Change

By Marleah Blades, Contributing Writer

"You have to create a strategic plan knowing that there's a high likelihood it will change. Does that mean you shouldn't plan? Absolutely not," says Mark Lex, Security Executive Council faculty member and former director of security for Abbott Labs. Over his career, Lex learned through hard-won experience that security strategic planning, done well, incorporates a balance of anticipation and response, detail and flexibility.

In today's business landscape, that balance is extremely difficult to strike. Perhaps that's one reason so few security and risk leaders succeed at effective strategic planning, and so many don't plan at all. Here are some other possibilities.

1. They don't understand it. There are plenty of capable leaders out there who didn't go to business school and who have never been asked to create strategic plans for their security departments. They are intelligent and motivated, but learning about strategic planning is simply not a priority, so it goes undone until management requires it. Then, under the gun, they create plans that demonstrate their lack of knowledge. "A lot of people don't understand the basics of what strategy is," says Lex. "It gets confused with goals. The goal is what you're planning to accomplish. The strategy is the how-to – how you are going to accomplish it. "

2. They've mystified it. Security strategic planning is no different from strategic planning in any other business function. Yet, because security leaders (and business leaders as well) have only in recent years begun to look at security as a business function, common practices like strategic planning have retained an otherworldly aura. Security is viewed as special or different – meaning exempt – because the function regularly conducts risk analyses and attempts to predict risk outcomes, making the SWOT (strengths, weaknesses, opportunities and threats) analysis included in strategic planning seem redundant. In short, strategic plans seem at best inaccessible, at worst irrelevant.

3. They don't know where to learn it. Security leaders with a business background are likely to be familiar with the basics of strategic planning. Bill Phillips, Vice President and Chief Security and Safety Officer for CNA, learned by running his own consulting business. "If we didn't have strategies for our business plans we just wouldn't have been successful," he says. Those without such experience may not know where to turn.

Libraries – particularly university libraries – generally have some good resources. A very few security seminars and leadership programs offer some strategic planning guidance. "I went to GSO 2010 several years ago," says Jeff Woodward, Senior Manager of Global Environmental Health, Safety and Security for Panduit Corporation. "That seminar really opened my eyes to strategic issues." James Connor, one of the organizers of GSO 2010, subsequently acted as consultant on a large project for Woodward, and he assisted in developing strategic plans to incorporate that project's results.

And then, there's always trial and error. "I learned by getting shot down enough times and going back to the drawing board enough to begin to figure out what I was doing wrong," says Lex. "Then I studied up and called upon colleagues and peers, contrasting and comparing with what they had done and beginning to develop some of my own ideas."

4. They don't take the time to do it. "I'm a very technical person, so it was hard for me to push myself away from day-to-day operations and delegate more in order to have the time to create a strategy," says Woodward. This is a common challenge, particularly when so many security leaders are being asked to do more with less –

money, staff and time. However, having that well-developed strategic plan in place will pay dividends on the investment of hours and effort.

STRONGER INFLUENCE AND BETTER SECURITY

By all accounts, a good strategic plan will earn the security leader credibility in the eyes of senior management. They are more likely to trust someone who has been proven a strategic thinker, and they will be more apt to ask him or her for counsel. The career implications of this boost can't be overstated, and neither can its impact on organizational protection. A leader with the ear of management is in a better position to propose and win support for far-reaching, security-enhancing initiatives.

The benefits of strategic planning also extend to the rest of the security staff and the strength of the entire function. "[My strategic plan] brought unity to the group that I was leading," says Lex. "There was a common language, goal, purpose, and really a common how-to in our approach. It helped tremendously in the cohesiveness of the group."

"It helps to develop the people within the department at all levels," states Panduit's Woodward. A good strategic plan is communicated all the way through the ranks and (directly or indirectly) sets performance expectations for each role, says Woodward. "It improves individual employees' performance in their jobs and makes the entire department stronger." In the long run, this all means better security.

Other benefits might include improved continuity during leadership changes (the management-approved plan gives new security leadership a point of reference for program development and focus) and support for staffing decisions (employee X is promoted over employee Y for her consistent contribution to meeting the department's documented strategic goals).

These benefits, of course, are only attained when the strategic plan is well-crafted. Some security professionals who jump the first hurdle and endeavor to write strategic plans miss the mark on the quality of the plans they develop.

> "The benefits of strategic planning also extend to the rest of the security staff and the strength of the entire function."

If a strategic plan is written in such a way that it cannot be approved, or that it cannot be followed, or if the writer doesn't actually intend to follow the plan but is only writing it to appease the boss, its utility will be limited, to put it lightly. In fact, it may do more harm than good. Focusing on two sometimes-neglected aspects of strategic planning might help avoid these pitfalls: alignment and flexibility.

ALIGN, ALIGN, ALIGN

A security strategic plan, like a strategic plan in any business function, must line up with the organization's strategic plan. The importance of this cannot be overstated. "Our goals have to be in line with the company's goals, because our main purpose is to support and enable the business," says CNA's Phillips. "So our strategies support and mirror the corporation's strategies. That's the first thing security folks need to get out front on." Because CNA's business, as the country's seventh-largest commercial insurance writer, is in risk and providing a marketplace for risk transfer, its security function draws goals and strategies around how to enable the business to be more effective and efficient in that mission. Says Phillips, "We examine operational risk, so our strategies are how we identify, examine and work with the risk the organization faces."

Alignment need not end with the organization-wide strategy, emphasizes Woodward. "The thing that's helped me the most is aligning to everything possible in the organization—core competencies, smart goals, service to employees, EHS programs, the lean program. We've aligned to our marketing strategy for our product, and that's helped a great deal in pushing our plans through and getting our capital approved."

Aligning means keeping connected to what the business is doing at all times. When the business changes or its plans change, an aligned function will ensure that its corresponding plans will change if necessary to remain aligned. This is where flexibility comes in.

Efficiency Versus Flexibility

Flexibility in strategic plans is valuable, but it must be paired with an ability to change quickly enough to follow revised plans or goals. Bruce Meglino, Professor of Organizational Behavior and Management at the Moore School of Business, University of South Carolina, remarks that there are steps organizations can take to increase their potential flexibility.

Before considering them, Meglino cautions, organizations must understand that increased flexibility inherently makes organizations less efficient. "The most efficient way to manufacture an automobile is on an assembly line," he explains. "Extremely efficient, but very difficult to change because they're specifically designed for that one purpose. There's a constant trade-off that organizations need to make between efficiency and flexibility."

The structural design of companies can make them more efficient or more flexible. "For example," says Meglino, "centralized decision making is usually thought of as having greater potential for efficiency, but it is very inflexible. Think about McDonald's compared to a local restaurant. McDonald's is very efficient but very inflexible. You can't walk in there and say, 'Let me have a hamburger with an egg on it.' They don't know how to react to that because it's not part of the protocol. A local restaurant, on the other hand, can be flexible enough to give you what you're asking for."

Hiring practices can also impact flexibility. "If you hire people with very specific talents targeted exactly to the job they're supposed to be doing, you're hiring for efficiency but not flexibility," Meglino continues. "If you set up cross training in an organization to allow employees to become broadly familiar with things beyond their job, that's an investment, as is hiring people with multiple skill sets. It's costly, but it increases the possibility that your organization is going to react to changes in its environment more successfully."

SECURITY AS A NIMBLE FUNCTION

The U.S. and international recessions, multiple wars, terrorism and political uncertainty have caused businesses worldwide to hunker down, says Bruce Meglino, Professor of Organizational Behavior and Management at the Moore School of Business, University of South Carolina. "Generally as things become more uncertain, organizations take a shorter-term view because they're not sure what's going to happen. Organizations abhor uncertainty," he says.

In an environment in which many companies are moving away from annual budgeting and toward rolling forecasts for many of these same reasons, according to a recent article in CFO magazine, a five-year strategic plan is rendered practically useless. Security strategic plans must be flexible.

"We need more anticipation, we need more business knowledge, and we need more nimbleness," says Lex. "The business executives who are best at strategy tend to design their strategies with several options. They're not willing to ride one strategy into the ground and crash and burn because it isn't working anymore. If they see their strategy isn't working, they apply some nimbleness and shift the strategy.

"For instance, you can lay out your budgeting based on last year's budget, but you also plan for a 30% contingency and a 50% contingency. In other words, what are you going to be able to provide to the organization if your budget's cut in half or


Marleah Blades

cut by a third?" asks Lex. This helps the security department shift gears quickly if the budget cuts come to pass, and in some instances it also helps the security leader defend against those cuts. If the executive staff asks the security leader whether they could expect the same level of service under such cuts, the security leader has an honest and documented answer prepared in his or her strategic plan.

Some security organizations have been successful by planning strategy at a less granular level in order to accommodate changes that impact the business direction or budget. This method must be used carefully, however, because if the strategy becomes too high-level, it may become vague and lose its ability to provide practical guidance.

The good news is that flexibility is one area in which security functions should have an advantage in planning.

"For security to be effective, we have to be forecasting," says Phillips. Monitoring and analyzing intelligence can serve the dual functions of risk management and business alignment through strategic planning, he says. The security function that is already collecting and analyzing intelligence on risks that may impact the business is more equipped to predict (and prevent where possible) business-changing events. In addition, security more than other functions should recognize the value of backup plans and business continuity.

Security leaders who carefully craft aligned, flexible strategic plans will reap the benefits of increased influence, greater effectiveness, and stronger departmental unity. If you haven't yet been asked by management to present your security strategic plan, don't wait. Begin now and ask trusted peers within and outside the business to assist you. SECURITY

About the Author:
Marleah Blades is senior editor for the Security Executive Council (www.securityexecutivecouncil.com/?sc=sm), which works with Tier 1 Security Leaders™ to reduce risk and add to corporate profitability in the process. A faculty of more than 100 experienced security executives provides strategy, clarity and proven practices that cannot be found anywhere else. To learn about becoming involved, e-mail contact@secleader.com.

Becoming an Expert in ESRM

By Brian J. Allen, Time Warner Cable

As a security professional, you should be an expert at managing security risks to your organization's assets, using risk-assessment processes to quantify and prioritize those risks. But do you work across all the business units of your organization to carry out those tasks? Do you ensure that there are mitigation-planning measures in place for the risks facing each of those units? Do you have the ability to challenge the business-unit-owners' risk acceptance when called for, and ensure that the appropriate-level person signs off on each of those risks? Those are the critical business skills that are at the heart of enterprise security risk management (ESRM), a holistic view of security that requires security professionals to work across their organizations – and to have the risk management intellect and business chops to challenge business owners and escalate risk conversations when necessary.


Brian Allen

ESRM is a seven-step process that begins with identification and assessment of the organization's assets. Identifying the security risks and vulnerabilities associated with each of those assets follows. Next is the quantification and prioritization of those risks and the development of mitigation plans. Security may undertake this step or assist business-unit owners with the plan development.

Mitigation plans may call for some or all of the risk to be accepted. This next step, risk acceptance and escalation, is where diplomatic and interpersonal skills come into play – because it's here that security has a responsibility to know when to evaluate and potentially challenge the business-owner's acceptance of the risks; to identify and involve other risk owners; and, to ensure that the appropriate person is signing off on the risk. That may mean understanding, for example, that the general counsel actually owns a risk that the HR department thinks belongs to them.

The next steps in the ESRM process are closer to the traditional security tasks of a security manager – incident response and investigation, conducting post mortems to look for root causes and then circling back to reassess the security risk to the company's assets, as them may have changed. This mix of security expertise, business knowledge, and understanding of risk management underscores the evolution of the skill-sets needed by the security professional of 2020.