SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Leadership > Next Generation Security Leadership >

The Nine Practices of the Successful Security Leader

Summary

In many professional fields such as legal, technology, and finance one can expect to find certain commonalities among the practitioners. These professionals share certain certifications or degrees, or they have progressed through a series of common steps or training regimens to reach their current position, where they share a fairly standard reporting level. The corporate security profession does not fit into such a mold. The Security Executive Council (SEC) has researched and studied the security community at a depth no other organization has, and the diversity of experience, responsibility, authority and background we've found is stunning.

However, across this varied landscape, commonalities of successful leadership do exist. Our community comprises many individuals who are recognized in the industry as highly successful security leaders. Because they have allowed us access to their time and insights, the SEC was in a unique position to uncover and identify similarities that contribute to strong performance.

A series of in-depth interviews in 2009 led us to identify nine practices that the most successful leaders have in common:

- The creation of a robust internal awareness program for the security department, including formal marketing and communication initiatives.
- Ensuring that senior management is made aware what Security is and does.
- Utilize a walk-and-talk methodology by regularly talking to senior business leaders about their issues and how security can help.

- Conversing in business risk terminology, not “security”.
- Understanding the corporate culture and adapting to it.
- Winning respect by refusing to exploit fear, uncertainty and doubt.
- Basing the Security program goals on the company’s business goals.
- Having top-level support from day one.
- Portraying Security as a connecting facilitator or coordinator across all functions.

Some of these leaders have worked to achieve these practices, such as creating internal marketing programs and conversing in business risk terminology. Others have come from luck or hard-won experience.

Methodology

We conducted in-depth interviews with 27 Tier 1 Security Leaders to discover and compare best practices. Most of the interviewees were leaders of the security programs in large corporations, most of which operate internationally. Questions put forth to them addressed issues such as the top risks to the organization (not specific to the security department), business alignment and drivers, internal influence issues, and senior management's view of the security function.

In the resulting qualitative analysis, the SEC’s Security Leader Research Institute researchers isolated commonalities reported among the leaders of the most successful, internally recognized security programs in the sample.

Results

Research shows that much of success revolves around communication and receptiveness. Each of our findings reflects how Security or the security leader is perceived by other business leaders, management and employees based on how the security leader presents risk and, to a great extent, him- or herself.

It should also be noted that many of these nine findings are intertwined with others. Ensuring management’s understanding often requires having a walk-and-talk mentality, for instance, just as conversing in risk terminology is beneficial to achieving business goal alignment.

The Nine Practices

The creation of a robust internal awareness program for the security department, including formal marketing and communication initiatives

A formal marketing and communications initiative builds internal awareness of the security department and raises the understanding of what security does and the value it imparts to the organization. This is not to be confused with a security risk awareness and training program. In this case, the successful leader knows that the security department is often not understood or that many employees do not even know there is one.

The marketing in this case, for example, involves having an internal logo and tagline for the security department (that is, “branding” the department), holding brown-bag lunches with security issues infused into them, regular newsletters on security department happenings, and encouraging and rewarding employee security champions.

When employees across the organization not only recognize the importance of security's contribution but become invested in furthering it, the security function’s potential for success dramatically improves.

Ensuring that senior/executive management is made aware of what security is and does

Management’s perception of Security impacts funding and organizational support for security initiatives and the security leader’s ability to influence risk-related decision making at a corporate level. This limits the effectiveness of the security function.

It will be difficult for corporate leaders to develop an accurate understanding of the organization’s security function without direct input from the security leader. Because the structure and operation of security differs from business to business, past experience at other companies may lead corporate leaders to a view of security that is unrealistic or erroneous in their present environment. In addition, because the security industry in general has done a poor job defining itself in a business context, many continue to assume that security begins and ends with guns, gates, and guards until they are shown otherwise.

Security leaders often fail to analyze their resource capacity regarding what the security staff is spending their time on and providing on a day-to-day basis. From this, what activities are valued by senior or executive leadership? Every other function needs to demonstrate where their time and resources are going -- why would the security department be exempt from this?

Several of the security leaders interviewed in this research hold seats in corporate strategy groups and on risk management teams and planning councils. Some hold C-level and VP titles with direct reporting to senior or executive management. These positions allow the security leaders greater access to communicate candidly and clearly with corporate leadership. High-level positions are likely evidence that management already understands and appreciates Security.

The security leaders interviewed who still sensed that management required greater understanding took the crucial step of speaking directly to business unit leaders to understand what security risk issues they were dealing with and what security services they find valuable. This is different than casual brown-bag activities. These one-on-one meetings often result in some kind of quantitative outcome that makes senior management aware of how their direct reports value Security's services.

Walk-and-talk methodology—regularly talking to business leaders about their issues and how security can help

The most successful security leaders we interviewed regularly speak to business leaders about their business goals. Sometimes it means taking the initiative to learn business processes, especially if no one volunteers to show you the ropes. As one leader stated, “I don’t wait for the phone call; I invite myself to major business meetings around the world.” In some cases, the security leader manages all these relationships himself; in others, deputies are charged with heading up regular communications with a select set of business units, making sure they understand their world and represent them in security plans.

These meetings are most effective when the security leader enters them with a business-first attitude. Security leaders begin by asking what senior or executive management wants and needs to accomplish, then present themselves as helpers in accomplishing those action items. Security does not set the agenda; the business sets the agenda.

Both these elements are critical to effective “walk and talk.” If a security leader tries to insert him or herself into regular meetings with senior management but ignores the second lesson on the tone and content of the talk, he or she may be viewed as arrogant or micromanaging.

Conversing in business risk terminology, not “security”

“We are business professionals who happen to be experts in security,” stated one of the leaders interviewed in our research. Interviewees remarked that they emphasized their role as “business assurance” rather than “security.” Some noted the importance of SWOT analyses and cost/benefit analyses within the security department to build better performance and to better enable the security staff to “talk business.”

The mission, goals, and strategies of the security function could be perfectly aligned with the business. However, if they are not communicated in the right terms, they may be rejected by senior management. Non-security business executives do not easily translate the language of security. Terms that describe security tactics, operations or projects may have double meanings—or no meaning at all—in business language. “Perimeter” has different meanings in corporate security and information security. “Convergence” is a commonly used term in many functions whose definition varies with its speaker. Even the word “risk” has a broader meaning for business (i.e., taking a calculate risk to enhance revenue) than for security.

Speaking about business issues in business terms helps enhance management’s understanding of security and increases the chances of management support.

Understanding the corporate culture and adapting to it

Many security leaders feel it is their job to change the corporate culture into something that is more security-centric. Our research showed that successful leaders believe the opposite: Their job is to learn the existing corporate culture and find the best ways to fit security into it.

An IT services company that prides itself on its relaxed and open philosophy is unlikely to appreciate a security leader whose focus is on locking the employee population out of newer communication technologies. Staff and management may look at that individual as a roadblock to be surmounted rather than a partner.

If on the other hand, the security leader talks with HR, employees, and management to learn what the corporate culture values most, then negotiates security policies and solutions that leave those values intact, the perception of that leader will be markedly different across the organization.

Winning respect by refusing to exploit fear, uncertainty and doubt

Respect is won over time, so this accomplishment requires long-term improvement and consistency. While tapping into the fears of business may seem the easiest way to gain support and elicit reactions, ultimately it results in a loss of influence and trust.

The successful leaders we surveyed focused on communicating security risk in business terms, as something to be transferred, mitigated, avoided or accepted—not feared. If the security leader is consistently level-headed in describing risks and their implications to the business, clear in conveying the options for mitigating the risk, and receptive to management’s concerns and decisions, they are likely to earn lasting respect.

Basing Security program goals on the company’s business goals

One of the most common terms in the interviews conducted in this research was “enable.” One interviewee stated, “Security enables the business to take risks—we don’t block them.” And another: “Our strategic plan is to enable the company to be the company.”

Many interviewed said that the goals and strategies of the security function cascaded down from the CEO. If brand protection was a major corporate concern, for instance, it became the priority of Security. Some security leaders who took this approach reported that management and other business units began coming to security to ask for assistance and advisement on various issues.

The security leader who puts the business first is more likely to experience long-term success than the one who works to drive the business in a direction set by security. There are several reasons this may be the case. When every function works toward the common goals of the business, setting internal goals that further the corporate mission, the entire organization should become more efficient and effective. This business optimization then reflects back on the individual functions, creating a cycle of higher performance and building success.

Communication is another factor. Basic psychology holds that a leader who is constantly asking "How can I help you?" will be met with less resistance and will be more positively perceived than one who is constantly interjecting "You can't do that." This positive perception easily translates into greater influence, always a factor in improved performance.

Having top-level support from day one

Those interviewed who started at an organization with a high level of management support performed best. They reported that if management places high value on the security department, then they are given one-on-one access to senior or executive management, and that their advice, if not always acted upon, is never ignored outright. The lesson here is to try to make this level of support a condition for your next career move.

The success of these leaders may be as attributable to their acumen as to the clear organizational focus on security's value. This finding should dispel any doubt of the correlation between organizational support and security success. To have such support is an enviable position in which few security leaders find themselves. However, a caveat: If your internal success relies on this relationship, you may be out the door when a senior or executive management shake-up occurs. Make sure the other practices are in place to thwart immediate displacement.

Portraying Security as a bridging facilitator or coordinator across functions

Every business unit in an organization is subject to, and sometimes owns, various risks. Many of the leaders we spoke with took it upon themselves to become central points of contact on risk for other business units. One stated that his organizational risk committee regularly sends information to business units to review and asks them to report back, ensuring they have an opportunity to make their voices heard.

Another remarked on his function's close relationship with no less than seven operational functions. That leader further stated that strong security requires these business units to be engaged in security risk management rather than periodically reminded of it.

When Security acts as a bridge between functions throughout the organization, it can help minimize redundancies and optimize resources. The security leader who focuses on achieving this also has the opportunity to identify, understand and respond to business unit risks more quickly.

What Does This Mean to You?

While our research identified nine common practices from the collective knowledge of industry-recognized leaders, no doubt there are more. Strive for the practices you can implement in your current organization or look for opportunities that may support these types of practices in the next phase of your career.

The extent of information sharing these interviewees offered for this study is unusual in our industry, but more such sharing is needed. The security function should share its wisdom to become a better understood, more highly recognized, and more valued contributor to an organization's bottom line. If you are at the tail-end of your career, consider playing a role in passing on your knowledge by sharing this report with your promising staff.

Visit the Security Executive Council web site to view more resources in the Security Leadership : Next Generation Security Leadership 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/