Leading Up

By Marleah Blades

How do you measure leadership success? Certainly, you can look down the chain and see whether your function and your team are accomplishing their objectives. You can usually tell if your staff is motivated and if they're eager to follow you. But strong leadership isn't just about how you relate to the people below you on the reporting ladder. It's also about how you relate to those above.

What your boss thinks of your performance and your function is an extremely important measure of your success as a security leader. It shows how well you're listening to the needs of the business as he or she articulates them. It also shows how well you're communicating your strategies to other business leaders. Both of these things provide a critical foundation for the success of the programs, policies and people you deal with every day.

Security magazine's May cover story ("What Your CEO Thinks") posited, based on their own research and the recent work of The Conference Board, that the top executives in many corporations have shifted their strategic focus in 2010. As the recession begins to ease, their greatest concerns are moving away from basic business survival issues back to innovation, profit growth,

Frank Brod, corporate vice president of Finance and Administration and Mike Howard, general manager of Global Security for Microsoft, are shown with other members of the global security team. Behind Brod and Howard are, front to rear, Grant Rauzi, Communications/Strategy and Finance; Denise Reubens, Risk and Background Investigations; Brian Tuskan, Operations, Investigations and Technology; and Charles Randolph, Intelligence and Executive Protection.

entrepreneurship, and building corporate reputation and customer loyalty.

The security and risk leader should be impacted by changes like these. As the strategic direction and business needs of the company shift, the security leader must recognize the nature of the shift and be prepared to open a dialogue with his or her boss on how security can help the company achieve whatever new goals it has set. The only way this will happen is if a strong relationship is already in place and the boss already sees you, the security leader, as a business enabler whose objective is to help the organization succeed.

We recently interviewed two successful security leaders at very different companies, along with their supervisors, to gain some insight into what that kind of relationship looks like and how it can be developed. Tim Baer, executive vice president, general counsel and corporate secretary for Target Corporation, and Frank Brod, corporate vice president of finance and administration for Microsoft, shared some similar thoughts about what they expect from their direct security reports, Brad Brekke (Target's vice president of assets protection) and Mike Howard (general manager of Microsoft Global Security).

BE A LEADER FIRST

Both the supervisors we spoke to view security as one of many business functions, noting that while it is a unique discipline, its leaders should be held to the same standards as all other business leaders.

"I look for the same leadership skills in all of my senior managers or leaders," says Brod. "I look for the ability to articulate a clear strategy, to provide motivational leadership, mentoring and coaching of employees, to drive towards impeccable execution of their work tasks and to motivate their group and provide the right rewards, recognition and feedback to help them grow in those roles."

Tim Baer ties the work of all Target's leaders, including security, to corporate goals and strategy. "At Target, we expect our executives to be creative in their respective disciplines, connect their strategies to the broader organization, and to be confident and self-reliant," he says. "Target leaders must be ambassadors for the company's goals and objectives and think critically about how their teams contribute to our success. Of course, we expect every leader to be an expert in their own business and share that expertise across the organization. But characteristics inherent to successful leaders – like innovative thinking and integrity – are commonplace among Target executives."

These executives expect all their direct reports to be leaders first, then experts in their fields. They view security leaders as business leaders. One of the reasons the security leaders in these two organizations have been successful is that they have viewed themselves the same way.

Since being named VP of Assets Protection for Target in 2001, Brad Brekke and his team have effectively overseen a remarkable broadening of responsibilities for the company's security function. Assets Protection once dealt primarily with traditional retail security concerns, such as shrink and physical security, and while those concerns remain a priority along with employee and customer safety, they now also have a voice in all decisions pertaining to global risk mitigation. Target Assets Protection has led the development of programs that have earned the company wide regional and national acclaim: Target & BLUE, a public-private partnership initiative through which Target supports public safety efforts, and the Safe City program, which unites local law enforcement, businesses and residents to reduce crime.

Mike Howard joined Microsoft as general manager of global security in 2002. In that time the company's employee population has more than doubled and Microsoft has increased its global footprint, adding locations in countries such as China and India. Howard has helped shift the perception of security away from guns and guards, building and communicating a strategy of global risk management, including internal intelligence and threat analysis. He has also leveraged new technology investments to generate revenue; Microsoft's Global Security Operations Centers (GSOCs), which provide central situational awareness and control over corporate locations worldwide, have become a showcase Microsoft technology. Security partners with Sales and Marketing to allow clients to tour the GSOCs to see what can be done with the technology available.

THE ROLE GOES BEYOND SECURITY

Mike Howard and Brad Brekke have both pushed the traditional limits of the security role, guiding their functions into the realms of value generation and reputation building. This is exactly the type of innovation their bosses expect of them.

Baer specifically emphasizes forward thinking and a tight pairing of security and corporate strategy as crucial elements of Brekke's success: "The role of the security leader is to be fully immersed in company strategies and key initiatives, understanding and anticipating existing and emerging risks and driving solutions to address them. The role of the security leader directly correlates with the success of strategic business initiatives."

Brod focuses on Howard's ability to build influence across organizational units through both his security responsibilities and non-security programs. "Mike has great influence across my staff, interrelating with leaders in other departments like real estate and procurement. He has outstanding educational skills; he reads and recommends management books for our people managers. Mike has also set up manager network rings, which bring together our people leaders throughout the organization in groups of 8 to 10. They meet every other month to network and to seek advice from peer managers on how to deal with shared issues."

Brod and Baer are certainly not alone in expecting more than traditional security from their security leaders. "The paradigm has been shifting in the last few years," says Howard. "If you're totally focused on security skill sets but you're not focused on risk mitigation or adding value to the business, as

How Does the Company See Security?

The Security Executive Council recently conducted an online poll asking participants "What best describes how you think your organization perceives your security department?" The results show that, if respondents' perceptions are correct, many organizations still see security as a drain on the bottom line, but just as many others see it as a way to add value. Most still lie somewhere in between.

Don't seem to know there is a security department	**4 percent**
They see the security department as a necessity	**51 percent**
They see the security department as a cost center	**18 percent**
They see the security department as a value center	**18 percent**
They see the security department as an enabler	**9 percent**

well as those core leadership skills and social skills that are necessary to help you navigate, you're not going to be as effective."

Research from the Security Executive Council backs up Howard's observation. The Council's 2007 report on *Security Leadership Background Trends* concluded that organizations were hiring more security leaders with backgrounds in business management and IT, whereas traditionally security leaders overwhelmingly came from backgrounds in law enforcement and military. Management was looking for a new type of security leader who could more easily add value through security and communicate risks in terms of business impact. The Council went on to develop the Next-Generation Security Leader model, drawing on research and the expertise of Council faculty, which identified six areas of knowledge that the security leader of the future would need to master. These include business and executive leadership.

NUMBER OF INCIDENTS IS NOT THE ONLY METRIC

Many security leaders measure the success of their programs primarily by counting how many incidents have occurred and determining whether the number is dropping, growing, or staying the same. While that is a valuable metric, Brod and Baer agree that in their organizations, it's not the only way to gauge security's success. "We measure performance against company-based metrics such as incident reduction, financial performance and productivity as well as team member and guest survey results," says Baer.

"Microsoft believes in commitments and accountabilities," Brod states. "So we have commitments for Mike and all our leaders. We expect impeccable compliance and execution. We also look at resource management. That is, how can we deploy the billions of dollars we have invested in facilities and 90,000 employees to provide security and access services in the most cost efficient and effective manner? We measure Mike also on his revenue influencing ability, and we measure the culture of respect and ethics. And in the end we're all looking to drive shareholder value."

Dropping the number of recorded incidents is great, but it's not enough. To be viewed as something other than a drain on the bottom line, security has to actually become something other than a drain on the bottom line, and they have to be able to show it. At Microsoft and Target, the security leaders are expected to uphold the corporate culture and create a rapport with internal and external customers, all while securing the organization's people and assets and building revenue opportunities.

PROACTIVE COMMUNICATION

After speaking with Brod and Baer, we discussed their thoughts with their security direct reports, Mike Howard and Brad Brekke. Neither was surprised by what his supervisor had to say. We asked them to share some of their secrets for staying so in synch with their boss's expectations. It all came down to maintaining formal, positive and regular communication.

"Open communication is vital," says Brekke. "We keep everyone informed and remain realistic about risks and what we can do to effectively mitigate them for the company."

Howard elaborated on how he maintains his seat at the table, stating that when Brod came on board at Microsoft, Howard's first objective was to meet with him to give him the broad overview of what security was and what it wasn't. This included a tour of the GSOCs. "We immediately got him to our GSOCs to get him up to speed on the totality of our technology, how it interoperates with other aspects of our business, and how it ties into the corporation," says Howard. After that initial overview, Howard and Brod endeavored to meet regularly at what Howard calls "monthly synch-ups."

"From a tactical and strategic standpoint I can talk to him and keep him up to date on not just what we're doing but what our strategies are," Howard says. "When I have quarterly business reviews with my team, I'll have Frank come out and speak. I've also made sure to synch up with other senior execs in the company – especially those I know he's going to be dealing with – because I never want him blindsided; I want to make sure everyone's on the same page."

Brekke also emphasizes the importance of company-wide awareness. "It's really important to have a seat at the table to be the voice for your team and keep the business informed of emerging issues and risks. That said, since one person can't be everywhere at once, team engagement is essential to communicate security strategies and keep a finger on the pulse of emerging company issues and initiatives."

He adds, "We work to build visibility into issues that impact the whole company—like safety or shortage – by leveraging dedicated communications resources and developing a culture where team members are cognizant

of the risks. Eventually, people embrace their role and become ambassadors for an issue. For example, we've built a strong culture at Target where people understand the importance of safe stores and communities, which is critical to our success."

Because there is always residual risk, it's critical to ensure that all senior leaders remain vigilant even when no major incidents are occurring, Howard says. "Once a month we put out an executive intelligence summary to people like Frank and senior leaders in the corporation so even if we haven't had to mitigate an incident in a month or so, they stay informed of the fact that there's a lot of stuff going on in the world that could affect our business and business continuity. They know that security has a piece of those issues and we're tracking them."

ARE YOU LEADING UP?

While the insights provided by Microsoft and Target shed light on some valuable lessons for all security leaders, they don't necessarily reflect what your boss expects of you. However, that doesn't make it less important for you to know what your own boss expects. How can you excel if you don't know what you're shooting for?

Can you easily and clearly articulate your boss's expectations of you and your function? Can you say with confidence that your boss understands and appreciates the scope of what you do? Are you certain he or she feels well informed of the security strategy and future direction? Have you been leading up the chain, or just down? SECURITY

About the Author:
Marleah Blades is senior editor for the Security Executive Council (www.securityexecutivecouncil.com), an innovative problem-solving research and services organization. To learn more about becoming involved, e-mail contact@secleader.com.

Making the Business Case for Security

What are the objectives of the Wharton/ASIS Program for Security Executives and how is it structured?

The Wharton/ASIS Program for Security Executives is about developing C-Suite business know-how and language. The faculty use cases, role-plays, and experiential activities to teach practical skills that reflect the latest research on leadership, finance, and strategy. While the academic content represents a diverse set of general management topics, the classroom discussions focus on the distinctive challenges of today's security executives. The participants themselves help guide these discussions, with experienced faculty asking probing questions about investments in security staff, programs and infrastructure.

The program design has evolved over six years, the result of a close collaboration between Wharton faculty and industry experts from ASIS International. After an initial week-long segment, participants return to work with leadership-oriented "application assignments," coming back to Wharton two months later to review results and partake in another week of classes. A secure website allows participants to interact with each other and the faculty during the two-month application period.

How can a CSO communicate a clear business case for investments in security?

Organizations face increasing threats to their security, while security budgets grow incrementally if at all. One reason for the growing gap between risks and resources is that security professionals use "insider" terms common within their specialties rather than the "language" that general managers speak, which is the language of revenues, costs, profits, and strategic positioning. The Wharton/ASIS Program teaches participants to speak this language and make cogent "pitches" for the resources needed to safeguard business continuity.

How would you differentiate the knowledge and experience required for a CSO in a leadership position in relation to other C-level executives?

A set of guidelines for the CSO, developed in 2004 by an international commission assembled by ASIS International, identified the core responsibilities and competencies of the CSO. In general, the commission concluded that the effective CSO must:

- Be more strategic than tactical in orientation, with exceptionally strong business and interpersonal skills.
- Understand the strategic direction and goals of the business and how to intertwine security needs with the goals and objectives of the organization.
- Possess a broad view of changes in the organization and environment that might affect security.
- Facilitate the use of traditional and advanced scenario planning techniques in assessing risks and threats to the organization.
- Demonstrate superior skills in communications, networking, interpersonal skills, planning, and managing capital expenditures.

The academic sessions of the Wharton/ASIS program reflect these capabilities: Strategy, Persuasion, Leading Change, Scenario Planning and Finance.

In the Wharton/ASIS program for Security Executive, a full day of the program is dedicated to the Gettysburg Battlefield Experience. What does this experience have to teach today's CSOs about leadership?

On June 30, 1863, Confederate General Robert E. Lee marched his army into Pennsylvania to engage General George Gordon Meade's northern forces. During the next three days, one of the great battles of the Civil War erupted, culminating in "Pickett's charge." The evolving strategies, command structures, and battlefield decisions of the Gettysburg struggle provide enduring leadership lessons for CSOs. These lessons suggest a leadership "template," elements of which include:

- Give your people wide latitude in pursuing their responsibilities, as General Lee gave his men, but not so wide that they fail to support the organization at critical times and places.
- Strike a balance, as did General Meade, between consultation and direction.
- Empower your direct reports to make strategic decisions, as did Joshua L. Chamberlain, regimental commander of the 20th Maine, and William C. Oates, regimental commander of the 15th Alabama, when they were defending Little Round Top, an extreme end of the Union line.

At Gettysburg, participants reflect on their own leadership styles and assess their ability to respond to ever changing conditions that mirror today's challenging business environment.