Tomorrow's SECURITY LEADER Today

By BOB HAYES and MICHAEL FICKES

[Originally published by: *Access Control & Security Systems*, Feb 26, 2007]

David Burrill believes that companies need security leaders in the C- suite working with the chief operating officer (COO), chief financial officer (CFO), the chief information officer (CIO) and other senior executives. Burrill also believes that chief security officers (CSOs) belong on the boards of directors of public companies and even qualify for promotion into the top job of chief executive officer (CEO).

"I think by 2020, it won't be uncommon to have a CSO on the board," he says. "By 2040, we may have a former CSO as a CEO."

Now a director of BurrillGreen Ltd., London, and the Emeritus Faculty Chair for international membership of the Security Executive Council, Burrill retired from the military intelligence service in 1992 and became head of security for the multinational conglomerate British American Tobacco (BAT). In 1998, the British Foreign Policy Center described the security organization built by Burrill at BAT as the benchmark or measuring stick for a multinational corporate security organization.

Burrill's approach to security differs dramatically from the conventional. To Burrill, protecting people and property is crucial, but it is only half the job. The other half is identifying and creating business opportunities for the company —just as the COO, CFO and other C- level executives identify and create opportunities.

Burrill is not alone. Many security leaders in the U.S. and around the world say that security today requires a range of skills that goes far beyond the capabilities of a traditional security director.

In addition to law enforcement and military skills, a security leader must understand his or her firm's business from finance and strategy to business continuity, competition and profits. The security leader must employ executive leadership skills appropriate to the corporation as a whole. He or she must be able to communicate, manage large projects, create strategies, assemble cross- departmental teams, execute plans and more.

A security leader must understand IT security and must maintain an awareness of emerging issues that may affect the company. He or she must follow legislative and regulatory trends, developments in globalization, trans- national crime, security research and development, and other trends that may one day alter the corporation's fortunes.

Today's most accomplished security leaders point to four general capabilities that define a modern security leader. First and foremost, a security head must understand his or her industry and company. Second, a security leader must develop a skill set that blends security, IT, business acumen and the ability to identify and evaluate emerging issues. Third, a security leader must change with the times and grow with his or her company. Finally, he or she must possess an imagination capable of exploring for opportunities that will add value to the company.

Security leader as business leader Randall Harrison, director of corporate security for Atlanta- based Delta Air Lines Inc. fits the emerging mold of security leader. Delta is the third- largest U.S. airline and the world's fastest growing international airline. Its planes fly to 304 destinations in 52 countries.

Delta executives wanted a Delta business leader to fill the security leader slot. Harrison has spent about 18 years at Delta. He came up through the ranks, starting in maintenance and then moving on to training, safety, environmental and special assignments. About a year ago, he was appointed head of security —not because of his security skills but because of his business skills.

One of the most fundamental skills that any senior executive must have, says Harrison, is the ability to create partnerships with diverse groups and individuals. For example, coming from the business side, he had to learn and get comfortable with the law enforcement side of security. When he started the job, he engaged a group of security consultants. Together, they interviewed 42 of Delta's most senior leaders, asking what security meant to them and what kept them up at night.

"These interviews changed my view of how the department would work," Harrison says. "The fundamental issue driving security now is creating value for the organization. How do we enable the organization to conduct business and meet its objectives?

"In the past, for example, security has been the ' go' or ' no go' decision maker," Harrison continues. "But that's not right. Security should identify threats and risks, outline measures that can be taken to mitigate the threats and risks, and engage management in the process so that they understand the impacts and can determine whether the end results are acceptable. This adds value to the organization."

Harrison also believes that measuring program performance adds value, and he has begun to measure things such as the number of investigations cleared, amounts of money recovered, workplace violence cases, compliance with regulations and so on. "If you don't measure performance, you cannot demonstrate value and you cannot instill continuous improvement and efficiency into the programs," he says.

Security leaders now coming from the business world
According to a recent survey conducted by the Security Executive Council, a membership organization of security executives from both the public and private sectors, more security people than ever are coming to their posts with business backgrounds like Harrison.

In the survey, 209 respondents were asked to describe their experience by selecting up to three different functions from a list that included law enforcement, military, information technology and various business operations.

Because people today typically hold more than one kind of job during their careers, many respondents selected two or three functions (three was the maximum allowed). As a result, the percentages in the survey results listed below add up to more than 100.

Law Enforcement: 37%
Military: 31%
Public IT: 17%
Business: 53%
Legal: 4%
Other: 20%

Blended skill sets
Today's security world has no defined career path, opening the door for executives with a wide variety of experience, notes Brad Brekke, vice president of Assets Protection with Minneapolis- based Target Corp. "You could have an MBA or background as a consultant or an IT professional," he says. "What's important is that you have a blended skill set."

Brekke has such skills. He focused on white- collar crime and public corruption as a special agent with the FBI, and upon leaving the Bureau, practiced corporate law and worked in retail management.

"Breadth of experience has helped me," Brekke says. "While law enforcement, security or IT knowledge is critical for a security leader today, you must also fully understand your company's business before addressing issues such as enterprise risk and risk management.

"This is elevating the profession. Traditional responsibilities are still there, but they have expanded and are now integral to business planning. Instead of strategy sessions with your technology expert and a guard supervisor, you are working closely with senior leaders and external partners to achieve key company business objectives."

What do blended skill sets mean in practice? Brekke points to his approach to crisis management planning. Traditionally, these plans dealt with nuts and bolts issues like evacuating buildings and coordinating company actions with the police. Of course, these jobs remain critical, but crisis management responsibilities now include new areas of expertise.

"We have crisis management plans for facilities," Brekke says. "And we also work closely with critical departments such as legal, internal communications, community relations and other areas to provide a comprehensive response to any event. Our partnership with internal communications, for example, was vital to our teams during Hurricane Katrina.

"Today, crisis management means building a team and creating a plan that is far more comprehensive than simply evacuating a building," he adds.

Some crisis management plans come with special technology. Brekke's team, for example, designed and supervised construction of a corporate command center where technicians remotely monitor Target facilities around the world. The command center also leverages technology with a weather service that can track weather by store location. His team also conducts drills to ensure the command center will effectively provide emergency services and coordinate recovery operations when the time comes. "You used to rely on an emergency management manual," Brekke says. "Today you have expertly trained people managing comprehensive plans and using state- of- the- art technology. It is far more sophisticated than ever. And it relies on people with blended skill sets drawn from across the company and a variety of industries."

As businesses change, so must security

Think about the massive changes that have rolled through the business world during the last 30 years. In 1980, desktop computers had only just begun to appear. IT security was a matter of locking the room holding the mainframe computer. Physical security was a matter of locking doors and patrolling corridors after hours. As years passed, and more computers appeared, business began to change —along with the job of security leader.

Richard Lefler, former vice president of worldwide security and CSO with American Express in New York and currently CSO Emeritus Faculty of the Security Executive Council, transformed himself as his job was transformed.

Lefler started with American Express in 1985 when security aimed to manage the financial risks to shareholders —by investigating crimes such as fraud related to the bank's credit card and traveler's check products.

While those tasks remain important, Lefler had much more to do by the early 2000s. "Over the years, as the business evolved, our security focus grew to include the protection of customers, shareholders, employees, our brand and our reputation," he says.

In the 1980s, security was aligned with business objectives. As business evolved so did the objectives and so did the job of security. "It is important always to keep security focused on or aligned with business objectives," Lefler says. "If your vision of managing security is not aligned with where the business is going, you will inevitably fail to return value to the company."

Business will continue to evolve and alter the responsibilities of security leaders. "Two issues will affect the future of a CSO," Lefler continues. "First, in the United States, the Department of Homeland Security is creating a set of standards for security professionals. There will be higher levels of compliance and regulatory oversight in security going forward. Consider, for example, the recent legislation enacted to regulate security in the chemical industry.

"Second, security is now reaching beyond the fence line," he adds. "In the past, a security director would be responsible, for example, for controlling shrinkage at a manufacturers distribution warehouse. He or she would install access control systems, video and alarms. This job is changing. Today, many third- party logistics firms are buying distribution warehouses, while companies are outsourcing logistics. Going forward, controlling shrinkage in the warehouse will require a security leader to act as an agent of influence over the third party."

That influence might come in the form of contract language that addresses security concerns, continues Lefler. A manufacturer, for instance, might make its distributor liable for shrinkage above a certain threshold, while requiring background verification for employees hired by the logistics provider.

Unexplored value

"What has always driven me is the idea that security is one of the last unexplored areas of value in an enterprise," says David Burrill of BurrillGreen. "Companies can profit from security through business enablement, enhanced reputation and better governance. In other words, security, like any other business area, can do all those things that turn on shareholders."

Here's a recent no- nonsense example. During the run- up to the war in Iraq, Burrill was still directing security for BAT. Burrill and senior corporate executives met to consider the security implications for the company's business efforts in the Middle East if and when war came. “We realized that a war would significantly limit our ability to get products to market in the Middle East,” Burrill says. “In anticipation, we extended our logistic capability, including increasing warehouse capacity in the region, and pre- positioned enough stock to see us through a crisis. Because we were in a better position than our competitors during the period of the war and following weeks, we seized market share.”

Security is still a tough business. But it is tough on an entirely different level than it used to be. For today's security leaders to succeed, they must know their companies and industries as well as any senior executive. They must develop skill sets that blend traditional security with IT security, business and the imaginative analysis of emerging issues. They must roll with the punches and change with the times. Last and most important, they must constantly apply their security background and sensibilities to the search for opportunities that will add value to the business.

- -

Bob Hayes is executive director of the Security Executive Council.
Visit https://www.csoexecutivecouncil.com for more information.

Rate yourself against the security leader of the future:

The following chart lists 65 knowledge elements that can enhance the success of a security leader today. The skills fall under six general "knowledge streams" that produce six different kinds of value for businesses.

Law enforcement and military backgrounds, for example, provide knowledge of investigations and prosecutions. IT security skills help in protection of critical information in both digital and printed formats. Business backgrounds help to align security value and business goals. A background career in corporate security ensures a security leader's intimate knowledge of a company,. Executive leadership skills produce a focus on business results. Awareness of emerging issues helps to maintain situational readiness.

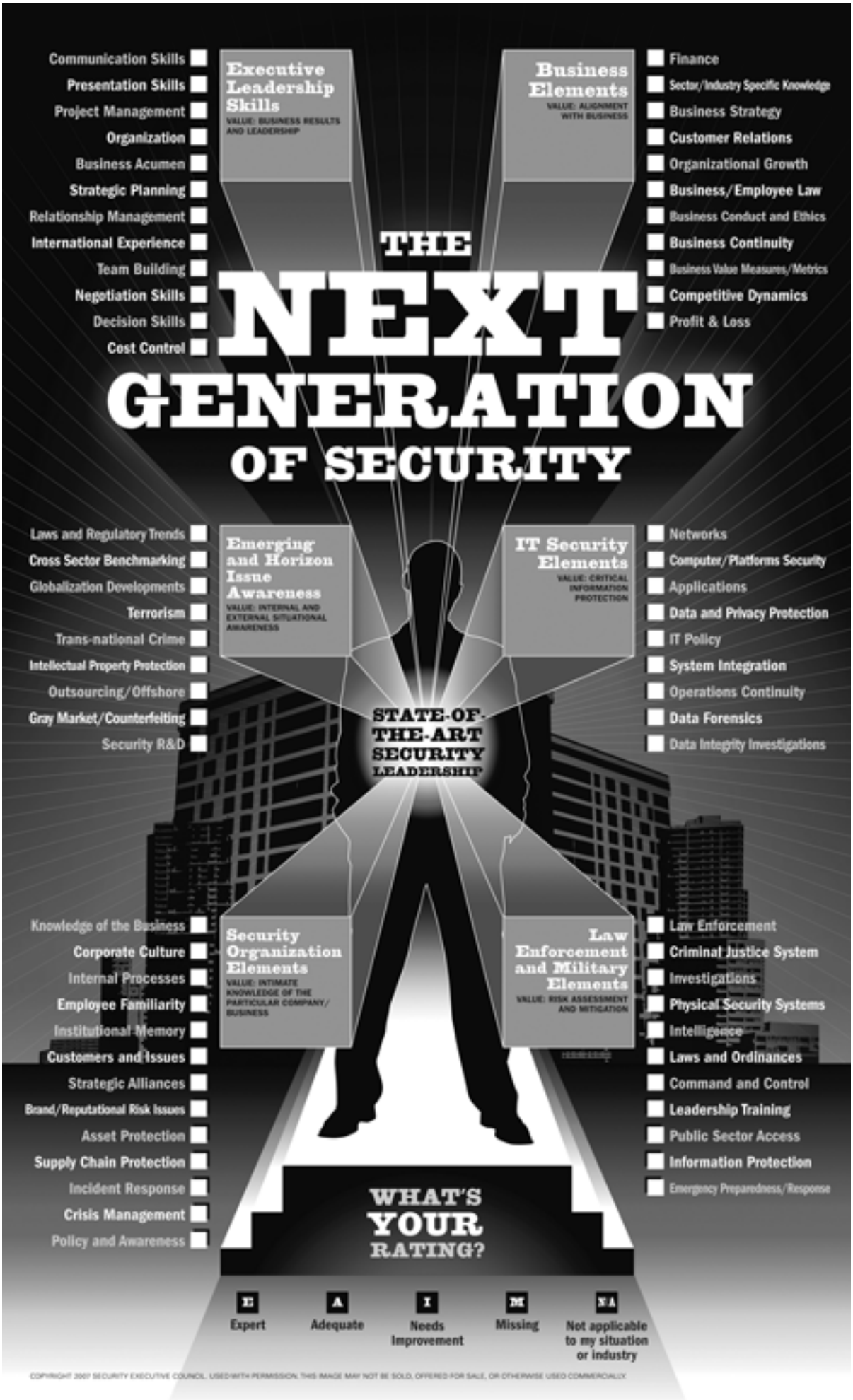
How well do you and your staff stack up to the security leader of the future? Try this self- test. Evaluate yourself against each of the skills noted on the chart. Give yourself three points for skills that you already possess (rate E for expert). Give yourself two points for skills that you can brush up on pretty quickly (rate A for adequate). For a skill that needs improvement, score 1 point (I for needs improvement). If there is a skill that you have no experience with and know nothing about, mark down a zero (M for missing).

When you finish, count up your points. Give yourself an additional one point up to a maximum of five points for every year of experience you have in one of the following fields: law enforcement, IT, business and security.

Divide your score by 2 to get your "Next Generation" score.

Those scoring 90 to 100 points can consider themselves ready to take on the challenges of 21st century security. A score from 80 to 89 points limits the role and level of your position in the organization. If you scored below 80, you may be risking your future. You should take steps now to expand your range of skills.

See next page for diagram ▶



COPYRIGHT 2007 SECURITY EXECUTIVE COUNCIL. USED WITH PERMISSION. THIS IMAGE MAY NOT BE SOLD, OFFERED FOR SALE, OR OTHERWISE USED COMMERCIALLY.