



What CEOs Think, 2011: Time to Jump on the Vision Bandwagon

By Bill Zalud
May 01, 2011



Bob Antin, CEO at animal hospital giant VCA, stresses comfort as a business strategy, while Charles Nicholls, his executive responsible for security, integrates that vision into the business sites.

Boss can be a noun or a verb. It can also be a cheerleader and partner with the aim of meeting and exceeding enterprise goals according to an organization's mission. Today, more than ever, enterprise security leaders are expected to focus beyond protection as chief executive officers and others in the C-suite assume, and rightly so, that their security colleagues get more from the security operation than just security.

Catch the vision.

For example, in order to get repeat visits, it's a matter of customer and staff comfort for Charles Nicholls, with security responsibility, to meet, according to Bob Antin, president and CEO of VCA, the world's largest chain of animal healthcare facilities.

For Mike Cummings, director, loss prevention services at Aurora Health Care, and Nick Turkal, M.D., president and CEO, Aurora Health Care, it's the consistent delivery of service in support of the organization's mission, vision and values.

"Our CEO's goals cascade down," adds Shawn Reilly, director of security for the Greenville Hospital System, about GHS President and CEO Michael Riordan.

Not every security leader has the confidence and rapport with his or her CEO and C-suite staff. But, as organizations evolve and grow, so does the role of security. In its fifth year, *Security* magazine has tapped into the thoughts of top enterprise management in terms of evaluation of their chief security officers and impact on the business. See the "CEO Report Card on Security – 2011" elsewhere in this issue.

As in previous years, the C-suite executives rate highest the effectiveness of their security operations to protect employees and property. And they rate as lowest security's efforts to grow the business and defend against litigation. In addition, as the economy slowly recovers, C-suite executives now focus on business management issues beyond survival. And that brings enhanced challenges.

Missing Best Practices Edge

In a separate survey of what CEOs think about their security executives, conducted by Steve Hunt of Hunt Business Intelligence, the industry analyst firm in Chicago, an entirely separate error CEOs spot in security organizations, according to his study, is a lack of management best practices. For example, "only the rare security executive is familiar with or strives to comply with Six Sigma, Baldrige, TQM or EFQM management practices," says Hunt. See the sidebar in this article with more thoughts from Hunt.

Such best practice strategies, some going back 20 to 30 years, have been in and out of favor for many enterprises but always a way to connect with the CEO. Respondents to the *Security* magazine What CEOs Think survey suggest the CSO would gain from a better focus on these strategies.

Six Sigma is a business management strategy originally developed by Motorola. It is used in many sectors of industry, although not without controversy. Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects (errors or security incidents) and minimizing variability in business processes. It uses a set of quality management methods, including statistical methods such as matrix analysis, and creates a special infrastructure of people within the organization. Security leaders included in the infrastructure gain from the attention.

The Baldrige program educates organizations in performance excellence management and administers the Malcolm Baldrige National Quality Award. Malcolm Baldrige was Secretary of Commerce from 1981 until his death in a rodeo accident. A part of the National Institute of Standards and Technology, it is a customer-focused federal change agent that enhances the competitiveness, quality, and productivity of U.S. organizations for the benefit of all citizens. It develops and disseminates evaluation criteria and manages the Malcolm Baldrige National Quality Award in close cooperation with the private sector.

TQM or Total Quality Management has been around since the late 1980s to retain or regain competitiveness in order to achieve customer satisfaction in the face of increasing competition. It's an integrative philosophy of management for continuously improving the quality of products and processes, including security.

TQM stresses the responsibility of everyone who is involved with the creation or consumption of the products or services offered by the organization. In other words, TQM capitalizes on the involvement of management, workforce, suppliers and even customers, in order to meet or exceed customer expectations, including those served by the security operation.

Especially for transnational enterprises with European presence, the EFQM excellence model is a non-prescriptive framework for organizational management systems, promoted by EFQM (formerly known as the European Foundation for Quality Management) and designed for helping enterprises in a drive to being more competitive. Regardless of sector, size, structure or maturity, EFQM measures where enterprises and their security operations are on the path to excellence; helping them understand the gaps; and stimulating solutions.

All of these approaches need to be addressed by enterprise security leaders through constant improvement, quality/excellence, measurement, and involvement by all stakeholders.

Measuring Up

Security can turn such management and measurement cranks but there is a little thing that complicates matters in the relationship of CSO to CEO, according to the *Security* magazine "What CEOs Think" survey. Call it change.

And when it comes to managing change by enterprise security leaders, CEOs and C-suite executives surveyed by Security's research firm, Maddy Associates, had some sage advice.

First, realize that significant change happens as a result of the courage and commitment of individuals. Then, believe that you have a unique purpose and potential. Security can make a difference for the entire business. From the big to the little things, from handling an incident to picking an IP video system, everything matters.

Commitment is essential as well as taking personal responsibility. “If it’s to be, it’s up to me,” said one CEO. Others pointed out that their security leaders should not get caught up in the how of things. Many things have been left undone because someone let the problem solving interfere with the decision-making. In addition, change is messy. There also is the need for awareness. When working with their security execs, CEOs and C-suite staff say that, when things go wrong, it is often that security was not aware of what’s wrong or what’s not working.

At the same time, security executives may not be aware of the CEO’s many roles beyond just being a boss.

Without a doubt, the CEO is responsible for the success or failure of the company. Operations, marketing, strategy, financing, creation of company culture, human resources, hiring, firing, compliance with security and safety regulations, sales, public relations – it all falls on the CEO’s shoulders.

But the CEO’s main duty is setting strategy and vision, a duty echoed by Cummings and other on-top-of-things security executives.

And it is security’s responsibility to both understand the strategy and vision and mold his or her program to those milestones. In addition, if vision is where the company is going, values tell how the company gets there. Values outline acceptable behavior. The CEO conveys values through actions and reactions to others. Values, according to the CEOs surveyed, are also at the heart of their security departments.

As compared to last year’s What CEOs Think survey, the economic downturn that pressured CEOs then is somewhat easing this year.

Easing Economy Brings More Pressure

As a reinforcing example, The Conference Board Measure of CEO Confidence, which had declined in the third quarter 2010, bounced back in the final quarter of 2010. The measure now reads 62, up from 50 in the previous quarter (a reading of more than 50 points reflects more positive than negative responses).

“The bounce back in CEO confidence signals that the cloud of pessimism that prevailed in the third quarter has lifted and CEOs are once again optimistic,” says Lynn Franco, director of The Conference Board Consumer Research Center. “The improvement in both current and future conditions suggests continued growth in the first half of 2011.”

As part of this What CEOs Think story, here are selected comments, observations and advice from some long-time security executives, many of them working in the healthcare industry,

which seems more exposed to risk management, strategic planning, community involvement, stakeholder and vision practices, as compared to some others.

VCA CEO Antin views security and teamwork with Nicholls as an essential way to grow the business of more than 520 animal hospitals in 41 states across the nation. These hospitals are staffed by more than 1,800 veterinarians. Many of the facilities operate late at night and in urban areas. “It’s a matter of comfort, feeling safe. There are many emotional situations and providing a comfortable environment is appreciated,” Antin says.

As a way to teamwork with his CEO, Director of Construction Nicholls, with primary responsibility for security, matches the corporate culture to technologies, policies and procedures. “Depending on the location of a facility, there are solutions we use such as intrusion and fire detection, access control, security video” and public view monitors in lobbies, so that clients and staff can see that protection is being provided. “Staff also has lanyards with panic buttons” in some cases and at some times.

To mirror the corporate culture, and since VCA continues to grow by bringing into the family existing independent animal hospitals, Nicholls seeks out local staff concerning their needs, their unique locations. “After hours, for example, some locations have two sets of doors so that a client can enter in from the weather and then be viewed and provided access through the second door.”

To add to the relationship of Antin and Nicholls, security service provider Protection 1 through Bryan Ahler advises and monitors where it makes business sense. Adds Ahler, “We are a first point of contact.” When a facility is brought into the VCA family, “we help audit the security system to see what is there.” And Nicholls works with his CEO to ensure that element of comfort at the operational, region, group and headquarters levels.

For Cummings, it all depends on the relationship between his operation and the organization’s president and CEO, Nick Turkal, M.D.

At Aurora Health Care, “I and my department have a great relationship based on the consistent delivery of service in support of the organization’s mission, vision and values over a considerable length of time. I and my leadership team, working through my boss, the senior vice president of human resources, strive to handle any issues or concerns forwarded from the president’s office and appropriately raise issues and make recommendations needing his approval through appropriate channels and with solid rationale.”

Building a Case for Expanded Security

An example: The adoption of certain aspects of a more robust executive protection program, not the least of which was target hardening of the corporate headquarters. Says Cummings, “Being a data driven organization, the case needed to be built around facts and not emotion. It was and the result was approval.”

He adds that “each year as my leadership team and I develop the plan for the department, it is filtered against both the organization’s mission, vision and values as well as the specific strategies and goals set by the CEO and senior leaders. For example, the last two years saw major building projects geared toward our growth in target market areas. All security related planning for these projects received high priority. We planned for the appropriate level of technology and staffing needed to support the opening from an on time and under budget perspective in consideration of the security needs of the site.”

The Aurora Health Care security executive also advises to think outside of the box when working with a CEO or president.

“While not directed exclusively toward the CEO, he or she will become aware in time if you understand and support the organization in nontraditional ways. Understand the culture and priorities of your organization and find ways to support it. Involvement in community outreach efforts that link to your organization, representing your organization on committees, local boards and charitable efforts that the organization supports demonstrates your larger understanding of what senior leaders value as well. Lending assistance with legislative or regulatory issues faced by the organization within your area of expertise can also be helpful in showing a greater understanding of what the organization needs. It is not always about the nuts and bolts of security.”

When it comes to approval for security technology, rarely do requests from the security department get to the CEO, comments Cummings. “Requests are generated based on sound business needs. That business need can be driven by regulatory requirement or pressure, the reduction of risk that the organization wishes to mitigate or a simple ROI around reducing costs or using less costly solutions (cameras or access systems as compared to staffing, for example).

“This part is simply being a leader within your organization understanding the business side and the organization’s main goal. In my case, it is about understanding that Aurora Health Care is in business to support the communities we serve by improving the health of the population and that everything we do in the security department needs to support that or we shouldn’t be doing it,” says Cummings.

For Anthony Notaroberta, director of hospital police at the New York City Health and Hospitals Corporation (HHC), the key to a solid security-to-CEO relationship is based on mutual trust and understanding for each other’s point of view, professionalism, and expertise.

HHC is a \$6.7 billion integrated healthcare delivery system with its own 385,000 member health plan and is the largest municipal healthcare organization in the country. HHC serves 1.3 million New Yorkers every year and more than 450,000 are uninsured.

Respect and Trust

“My CEO respects my expertise and position on issues, especially if and when it may conflict with hers. Although we both work to ensure patient safety and satisfaction, I have a specific area of operational concern where hers is much broader and involves many more intermingled issues

throughout,” Notaroberta says. “However, even when she makes a tough decision, directly or indirectly against my position, based on her respect for my reasoning, expertise, and rationale and the willingness to seek out my opinion on matters, I can support her decision no matter what the direct outcome towards my concern.”

Concerning the security mission and strategies, Notaroberta says, “Our goals and visions have many mutual components. For example, the highest prioritized goal for patients here is patient safety. My CEO has made patient safety the highest priority for everyone in the facility and we, as a major contributor towards this goal, facilitate the objectives by focusing our departmental functions in and around the hospital’s goals.”

When it comes to security technologies and services, Notaroberta starts with stakeholder buy-in “including committee meetings, subject matter experts, and industry recognized standards, all involving direct communication with people in these areas. Once services are decided upon, the presentation to the CEO is made showing benefits to patients, benefits to hospitals, and any downside in moving in this direction. Nothing is hidden. All pros and cons are discussed up front; and a professional decision is made.”

At Greenville Hospital System University Medical Center (GHS), Shawn Reilly knows his property is more than just buildings. It’s a multi-faceted group of physicians, nurses, teachers, researchers and other highly-skilled, highly-specialized medical professionals committed to providing the best possible health care for a healthy lifestyle.

When it comes to working with the C-suite, Reilly, chief of police and director of security, says that, first, his CEO is not insulated from any of the 10,000 or so employees. “He has opened a variety of communication lines that allow anyone to get their thoughts and opinions to him: annual employee surveys, quarterly town hall meetings (14 of them each quarter), direct email, CEO corner on our Web site just to name a few. He schedules regular meetings with me – most at 5:00 am – to see how we are doing taking care of night shift employees. He also personally tests our emergency call boxes and security response times along with employee escorts.”

Reilly boils down to one word the key to a successful relationship between security and the CEO: honesty.

Support and Service

“But it goes beyond the CEO; security is part of [the overall] service and support function and that is just what you need to do – support. If you are saying no to other directors and employees when they ask for help or changes to procedures to improve efficiency, you’re saying no to the CEO. You can’t always say yes, but you can listen to their needs. When you can make the job easier for others, you’re adding to the bottom line of the organization and that gets back to the CEO.”

Reilly and his CEO also share a clear understanding of the people in and around their facilities. “As you can guess, security goals are focused on people and service pillars. Getting people safely and quickly to and from work is a big deal in an industry that operates 24/7 and is 85

percent female. Our CEO relates employee satisfaction to a successful business. Also a reputation of being a safe place is important for our patients and visitors.”

Last year, Reilly’s relationship to his C-suite colleagues was put to the test. “During 2010, a rather tough year for everyone, I proposed we create our own police force. It really took all of our corporate leaders to be on board to get laws passed and establish our own jurisdiction. Surprisingly, [the CEO] was the reason that, at 54 years old, I agreed to take on the role of chief of police and attend the South Carolina Police Academy. The amazing part is not that he has interest in and works with me, but he also gives the same attention to everyone else in the organization.”

CEO REPORT CARD ON SECURITY 2011

Chief executive officers, presidents, chief operating officers and chief financial officers rate their security operation in 14 key areas.

Crucial Business Needs Impacting Security

	2007	2008	2009	2010	2011
Protecting Employees	A-	A-	A	A-	A
Maintaining Business Continuity	B-	B	B-	B	C+
Working with Other Internal Departments	C	B-	B	C+	B-
Protecting, Enhancing Brand, Reputation	C-	C-	C+	B-	C+
Execution of the Security Plan	N/A	C	B-	B-	B+

Essential Business Needs Impacting Security

	2007	2008	2009	2010	2011
Complying with Regulations	A-	B	B	B-	B-
Securing Property	A	A	A	A	A
Limiting Financial Risk	B	B-	C+	C+	B-
Protecting Confidential Information	C-	D	B-	C	C+
Protecting the Supply Chain	D	C-	C+	C	B-

Important Business Needs Impacting Security

	2007	2008	2009	2010	2011
Enforcing Ethics	B-	C	B	B-	B-
Defending Against Litigation	C	C	B-	C	C
Reducing Insurance Premiums	C	B-	B	B	B-
Helping Grow the Business	D	C	C+	B-	C

Source: A mail and email survey of 100 CEOs, presidents, COOs and CFOs of enterprises with a formal or stand-alone security department. Conducted Feb. 15-Mar 15, 2011 by Maddy Associates.

About the CEO Report Card -- Surveys were sent to Fortune 1000 and other company CEOs, presidents, chief operating officers and chief financial officers with a promise to maintain confidentiality of responses. Companies had to have a staffed security department, operation or established staffer. The respondent companies range from \$410 billion to \$95 million in revenue, from 2.5 million employees to less than 700. Enterprises range from retail, manufacturing and transportation to government, utilities, healthcare and educational institutions.

A Sharper Focus on What CEOs Think

Steve Hunt of Hunt Business Intelligence, the influential industry analyst firm based in Chicago, recently performed his annual research on what the CEO thinks.

Among findings, relates Hunt:

“CEOs think security executives are excellent security managers but downright rotten business people. Specifically, CEOs complain that security executives still have the mentality of ‘keeping bad things from happening’ rather than the more business-minded approach of ‘adding value to the business.’

“An example of where security executives often stumble is how they misuse ROI,” contends Hunt. “Return on investment is a common tool in the toolbox of every executive, along with total cost of ownership, annualized loss expectancy, and cost-benefit analysis. The trouble with ROI is that it is too simple. The idea of calculating an ROI is to measure the difference (the ‘delta,’ in management-speak) between apparent cost and apparent benefit. Therefore, when comparing two products, you would look for the one that offers the greatest delta between cost and benefit. Simple, right?”

He adds, “Security managers, who have had no training in business management, easily fall into that ROI trap.

“Here’s the trap. Solving a security problem under budget is not a matter of ‘finding the best deal.’ It is a matter of solving the problem most cost-effectively. To do that, an executive should first measure the degree to which a product or project solves the problem or achieves the goal, and then find the most economical route to attain it. A large ROI may demonstrate that you are getting a lot for your money, but it in no way measures how close the product gets to solving the problem you’ve set out to solve.”

Hunt continues, “It gets worse. By focusing on and making decisions by ROI, an executive will always be at risk of purchasing products that do not solve the problem. Which in turn, will mean that the products they do buy will seem unsatisfactory. Which, in turn, will drive more spending and more errant ROI calculations to solve the problem that still is not solved.



Business management and measuring performance are among the keys to working more closely with the CEO, says Steve Hunt, the influential industry analyst.

“An entirely separate error CEOs spot in security organizations is a lack of management best practices. For example, only the rare security executive is familiar with or strives to comply with Six Sigma, Baldrige, TQM or EFQM management practices. The book – Good To Great (by Jim Collins, who answers a single question: Can a good company become a great company, and if so, how?) – is the best introduction to these concepts. In a word, it means the disciplined approach toward continual improvement. Are all of your security processes documented? Does every employee feel empowered and motivated to improve every process?”

Risk Management: The Glue Between the CEO and CSO

Moving beyond card access, intrusion and security video, enterprise security leaders will gain by moving into the C-suite level of risk management. Here are a few questions that The Conference Board poses to its CEO members and that can apply to the CSO.

- How can companies move toward more risk management solutions that are not merely compliance-driven?
- How are companies reorganizing to achieve effective risk management?
- How can enterprise risk management or ERM become part of corporate strategy and tie in with performance management
- How can a company proactively manage reputation risk?
- How are companies managing risks within their supply chains?