A Seamless Alliance

The CEO and Security Executive at Baker Hughes Inc. discuss the elements of successful collaboration.

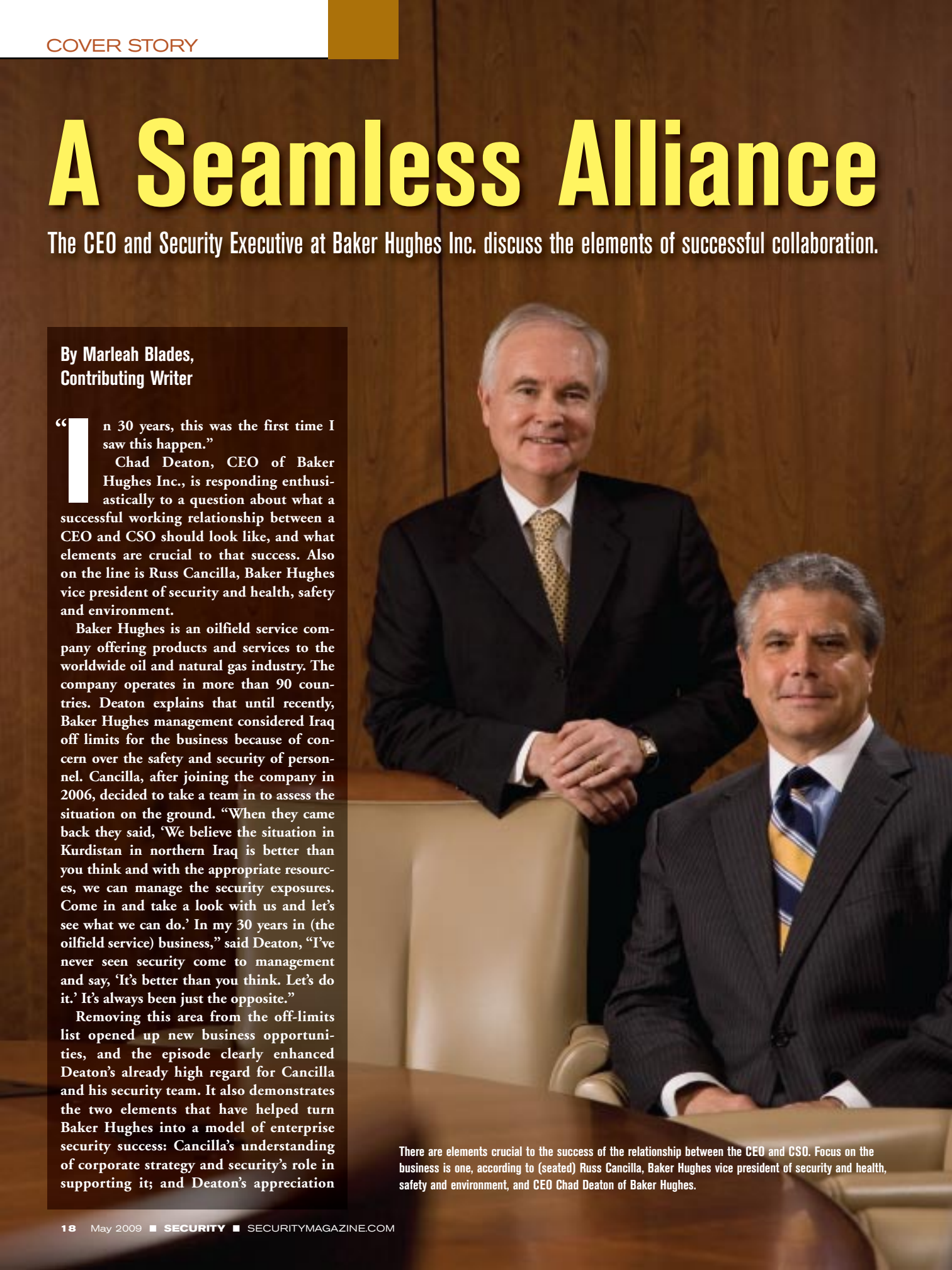
By Marleah Blades, Contributing Writer

"In 30 years, this was the first time I saw this happen."

Chad Deaton, CEO of Baker Hughes Inc., is responding enthusiastically to a question about what a successful working relationship between a CEO and CSO should look like, and what elements are crucial to that success. Also on the line is Russ Cancilla, Baker Hughes vice president of security and health, safety and environment.

Baker Hughes is an oilfield service company offering products and services to the worldwide oil and natural gas industry. The company operates in more than 90 countries. Deaton explains that until recently, Baker Hughes management considered Iraq off limits for the business because of concern over the safety and security of personnel. Cancilla, after joining the company in 2006, decided to take a team in to assess the situation on the ground. "When they came back they said, 'We believe the situation in Kurdistan in northern Iraq is better than you think and with the appropriate resources, we can manage the security exposures. Come in and take a look with us and let's see what we can do.' In my 30 years in (the oilfield service) business," said Deaton, "I've never seen security come to management and say, 'It's better than you think. Let's do it.' It's always been just the opposite."

Removing this area from the off-limits list opened up new business opportunities, and the episode clearly enhanced Deaton's already high regard for Cancilla and his security team. It also demonstrates the two elements that have helped turn Baker Hughes into a model of enterprise security success: Cancilla's understanding of corporate strategy and security's role in supporting it; and Deaton's appreciation



There are elements crucial to the success of the relationship between the CEO and CSO. Focus on the business is one, according to (seated) Russ Cancilla, Baker Hughes vice president of security and health, safety and environment, and CEO Chad Deaton of Baker Hughes.

for and awareness of safety, security and business risk.

A SHARED FOCUS

Deaton joined Baker Hughes in late 2004 and brought Cancilla on board as CSO in mid-2006, reporting to the general counsel. Before that time, the corporate security function at the company worked independently from security operations teams. In fewer than three years, Cancilla restructured corporate security into an enterprise security and crisis management (ESCM) function built around a security business model. The move to ESCM has improved the planning, execution and management of security programs enterprise-wide and better aligned security activities with Baker Hughes' business model.

Among other changes, Cancilla has also helped develop a security assessment process that requires all security personnel to conduct standard business S.W.O.T. (strength, weaknesses, opportunities and threats) analyses to identify emerging markets and opportunities and assess risks. Russ Cancilla is a member of the Security Executive Council.

Improvements like these led to Cancilla's promotion in January, by which the company combined the functions of security and health, safety and environment and brought them under him as corporate vice president. Now he reports directly to Deaton with a seat on the corporate strategic policy council.

Deaton believes the change just made common sense. "We have a significant number of people all around the world. In this oilfield service sector, like any multinational, we have a lot of exposure. And as we move into countries that sometimes have a lot of problems; it's critical that we look after the security and the safety of our people, which are closely linked. It's very important for us to make sure the senior management team understands the risks we're faced with," he said.

Cancilla's impressive performance as CSO clearly paved the way for strong future collaboration with his CEO. In order to continue the successes that have brought them this far, Deaton and Cancilla must maintain a common and articulated focus on the well-being of the business.

BUSINESS FIRST

"I expect our CSO, just as I expect our CFO or General Counsel, not to focus on only his particular function but to look at strategy in general," said Deaton.

It's an expectation Cancilla shares, both of him and, at another level, of his entire security team. "We look at the security team as a group of business professionals who happen to be expert in security," he said. "In a very, very unusual circumstance should security ever say a business can't do a given thing. We're a support function. Our objective is to understand what the business wants to do and figure out how we can support it. It's generally just a matter of how much risk we want to accept and how much investment we want to make into security."

One key to this approach is knowing how to communicate the impact of risk in the language of business. "We have to be able to demonstrate that we understand what ROI means and what a S.W.O.T. analysis is and why presenting a business case analysis is important. Then we must apply those principles to demonstrating the cost and benefit of a security decision. We have to be able to use those terms and imperatives when we're talking about security," commented Cancilla.

"It's easy to say security is adding value to the business. But really, is it? As the leader or CSO, you don't have to be an MBA, but you can't come into the boardroom or the senior executive meeting and talk about just security. You have to be able to talk about why or where there is value in terms of real dollars." This also means the security leader must remain focused on the overarching business objectives. He or she must bring to a strategy meeting the information that is relevant to the decisions being made and demonstrate how the security input is relevant in business terms.

Often business leaders need some coaching on how and why it is important to include security as a business function. When security has long been viewed as an obstacle, as it was by many at Baker Hughes before Deaton and Cancilla came on board, managers and business leaders may have a hard time remembering that the security team is really there to work for them, not against them.

"There's one thing I ask of our business folks here," Cancilla observed. "If one of our security professionals tells you we need to invest in a security program, please don't let the first question be 'How much will that cost?' Instead, ask 'What's the risk or threat?' Then you have an understanding of why there might be an investment needed to manage that risk or threat, and you as a business leader can make a more informed decision on whether to invest that money."

BUILDING TRUST ACROSS THE ORGANIZATION

Deaton says focusing on the business is the primary action Cancilla can take to help them maintain a strong working relationship. The second is satisfying the leadership at all levels all across the company.

"I think it is critical for any senior executive to be accepted by the thousands of employees we have around the world," said Deaton. "Our operations people have to see that Russ or any other executive is bringing value to them, that they're solving their problems. And Russ has done that. When he came on three years ago, security was there but it was kind of obscure. It was looked at as a cost, as overhead, but Russ and his team have changed that. Our operations people want him there, they want his opinion, and they want his team's opinion, so they go to them to help them solve a problem."

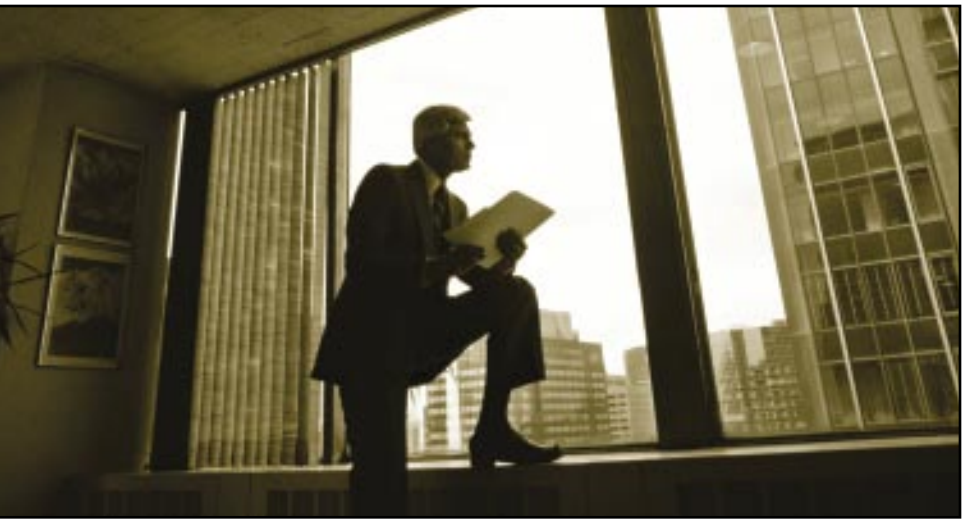
> "A security awareness process brings together the CSO and CEO."

Cancilla agrees. "I don't think it's just the relationship the CSO has with the CEO that matters," he says. "I think it's the feedback the CEO gets about what the security organization is doing. And if those relationships aren't strong and you don't have credibility, the CEO may have to say, 'I like you, but are you really bringing anything to the executive table that translates into helping us make better decisions or be more successful?'" SECURITY

About the Author

Marleah Blades is senior editor for the Security Executive Council (SEC). The Security Executive Council is a member organization for senior security and risk executives from corporations and government agencies responsible for corporate and/or IT security programs. In partnership with its research arm, the Security Leadership Research Institute, the Council develops tools to help lower the cost of members' programs, making program development more efficient and establishing security as a recognized value center. For more information and inquiries on membership requirements, visit www.securityexecutivecouncil.com/?sourceCode=secmag.

A Strong Relationship...Except



CEOs are shifting their focus in an economic downturn. Crucial are protecting employees, maintaining business continuity, working with others, protecting the firm's reputation and execution of the security plan.

By Bill Zalud, Editor

Except for the economy. There's a solid partnership story, in the preceding story in this issue, as Chad Deaton, CEO of Baker Hughes Inc. works with Russ Cancilla, Baker Hughes' vice president of security and health, safety and environment.

Still many CEOs and C Suite executives have another fish to fry today. It's called survival.

That doesn't mean they don't appreciate their security executives and the operation of it. And they see growing value in security as a business tool. It is really more up to the chief security officer or security director to make a new case.

Annually, Security Magazine surveys 100 CEOs and Presidents asking them to score their security operation in 14 categories. This year, they were also asked to label the importance of those 14 elements from critical and essential to important.

BIG BOSS RELATIONSHIP

Also interviewed were top security executives as to how they perceive their relationship with the big boss.

For security executives, it comes down to trust and confidence.

Chris McColm, CPP, corporate security manager, Manitoba Hydro and Gas, said, "I believe CEOs typically view the security operation as an internal insurance policy."

He added, "Our CEO has displayed his support for our program by ensuring that we are complying with security standards in the industry and ensuring that we are protecting our critical assets by providing reliable electricity to our customers in Canada and the U.S. The most important elements between the top security executive and his CEO are trust and confidence. If a CEO can trust the decisions being made by the security executive are in line with corporate business ethics and policy, then the CEO will be confident that the security executive is protecting his corporation's assets. This goes far in the boardroom when security is asking for money to spend on certain projects or events."

Protecting assets is – today – a shared responsibility and a top one. Protecting employees is both a crucial mission and one that is done well, according to the 2009 What CEOs Think of Security survey by Security Magazine.

As in most relationships, solid communications is essential. Mike Cummings, CPP, director, loss prevention services, Aurora Health Care, said, "We who are responsible for the security function must be strong communicators around what risks we have identified and how we are or need to mitigate those based on the organization's best interest. We need to be visionary and able to see how we align with where the organization is going and be able to communicate options whenever possible with clearly identified benefits and challenges associated with each option."

IT STARTS WITH THE CEO VISION

"The CEO needs to communicate the direction the organization is going and expectations around the role security plays. The CEO must also communicate the final decisions clearly, preferably with reasons so the CSO can support and use the reasons as a guide to how the decision is executed and a learning of how the CEO makes decisions. This should not be any different than he or she would do for any other important department. The other element would be trust, which will develop over time if the above takes place," added Cummings.

Charles Smith, corporate director, protective services at OhioHealth, agrees. "The most important element between the top security executive and his or her CEO is to have an open relationship where the security executive can go to the CEO with an issue when it is important for him or her to know, rather than have to go through several layers to get the information to the top level. There must be mutual respect that flows both ways so that the CEO is comfortable sharing confidential information with the security executive."

Protecting and enhancing the brand and reputation are also rated as a crucial mission shared by security; but CEOs rate performance lower in the Security Magazine study.

A growing number of major global companies are investing substantial resources to manage their reputation risk and have increased their efforts to do so over the last three years, according to a report by The Conference Board, the global business research and membership organization.

"Safeguarding reputation is even more critical today because companies have developed successful ways to make reputation risk management part of their overall risk management," said Ellen Hexter, director, enterprise risk management at The Conference Board and co-author of the report with Sandy Bayer,

president of Bayer Consulting. "In addition, different stakeholder groups are becoming more sophisticated in how they drive corporate reputations. Critics on the Internet can now transmit their opinions and complaints around the world with ease. Most importantly, consumers have high expectations that companies will not only produce quality products and services, but also will act ethically in their creation and distribution."

PROTECTING REPUTATION MORE IMPORTANT

Rick Harris, senior director safety, security & environmental services, Orange County (Florida) Public Schools, has a keen eye on reputation. "It's essential to have immediate access to the boss regarding time sensitive issues, especially those that may generate negative publicity about the district or internal programs and activities."

The Conference Board defines reputation as how a company is perceived by each of its stakeholder groups and reputation risk as the risk that an event will negatively influence stakeholder perceptions. Many reputation risks are the secondary result of other, more traditionally recognized risks. For example, if a manufacturer produces an unsafe product, it may lose customers and is likely to suffer financial costs due to a product recall, both of which impact reputation. Reputations may be damaged for any number of reasons, including that stakeholders perceive a company to be unethical.

Workplace violence incidents can also bang up reputation. Check another article in this issue on workplace violence and its impact on the enterprise.

"Although reputation is the quintessential intangible asset, a strong corporate reputation yields concrete benefits - higher market value, stronger sales, and an increased ability to hire the best and the brightest," commented Bayer.

The report is based on the findings of The Conference Board Reputation Risk Research Working Group and a survey of 148 risk management executives of major corporations. More than three quarters of the respondents to the survey said their companies are making a substantial effort to manage reputation risk (82 percent) and they have increased focus in this area over the last three years (81 percent).

REPUTATION IS EVERYONE'S BUSINESS

Other key findings:

Reputation risk should be managed throughout the organization. Although communication is of critical importance in responding to a risk event, a company's reputation should be considered during the preparation and execution of strategy and new projects, which hasn't been the case in most companies.

Reputation risk is often not incorporated into risk management. Only 49 percent of executives surveyed said that the management of reputation risk was highly integrated with their enterprise risk management (ERM) function or another risk oversight program.

Assessing reputation risks is a top challenge. Fifty-nine percent indicated that assessing the perceptions and concerns of stakeholders was an extremely or very significant issue, making it the highest-ranked challenge.

Media monitoring has become more sophisticated. Today, there are tools to assess whether coverage is positive, neutral or negative; the credibility of publications; the prominence of coverage, etc.

Efforts are being made to quantify the value of reputation. A select group of companies is making progress in this area by working with specialist consulting firms to quantify the impact of reputation on share price.

Social media are gaining influence, but most companies are ignoring them. Although consumers and investors are increasingly gathering information from blogs, online forums, and social networking sites, only 34 percent of the survey respondents said they extensively monitor such sites, and only 10 percent actively participated in them.

"Boards of directors, senior management, and operating management should demonstrate an active commitment to strong reputation management," concluded The Conference Board. "While crises are sometimes inevitable, a company's reputation when it is most vulnerable and how the organization responds can have an enduring impact for years to come."

DOWN TO STRATEGIES

Of course the heart of asset management is the strategies of the business.

Observed Craig Kramer, director of public safety/security at Advocate Condell Medical Center, "It's the responsibility of the security leader to get involved in the overall strategy of the organization and show how security is a value added department. You must support the strategy in a cost effective manner and ensure that leadership understands the overall risks the organization faces. Leadership also needs to know what are the measures and cost (ROI) to eliminate or reduce those risks. If you cannot do that, then security becomes a necessary evil and cost adder."

For Kramer, it's a one-to-one equation.

> **"The key: trust and communications between CEOs and their security leaders."**

"To have an open discussion on what the CEO feels are areas at risk or areas they would like shored up is important. It all comes back to the bottom line and how we add to it or protect it, plus maintaining the organization's reputation."

But no matter the relationship of CEO to security today, the economy is more than a little speed bump. The Ken Blanchard Companies annual Corporate Issues Survey, for example, shows that at the management level, there has been a significant shift to challenges more focused on people development — creating an engaged workforce, managing change, and developing potential leaders. And at the employee development level the top three issues include performance management, managerial/supervisory skills, and interpersonal communication skills.

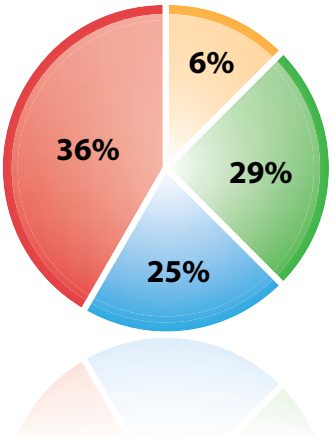
Respondents were asked to describe their organization's overall outlook in regard to the economy. About a third (29 percent) of respondents is optimistic — believing that the economy will begin to improve about midway to two-thirds of the way into 2009. A little more than a third (36 percent) is only slightly optimistic — believing that the economy will not begin to improve until the

third or fourth quarter of 2009. And a quarter (25 percent) of respondents were not optimistic that the economy would begin to show signs of improving until 2010.

TOUGH ECONOMIC TIMES

It's apparent that this year and next will be a tough time for the CEO and the security leader in his or her organization.

Rio Rancho Public Schools' Mike Tarter, executive director safety & security, speaks for many colleagues. "I love my job! However, this year has been rough and next year looks worse. We will have to adapt, overcome, and improvise like we never have before." It's the same for the boss.



C SUITE EXECUTIVES: WHEN WILL AN ECONOMIC RECOVERY OCCUR?

In Q1/Q2 of 2009	6%
In Q2/Q3 of 2009	29%
In Q3/Q4 of 2009	36%
Not until 2010	25%

Source: Ken Blanchard Companies

In the Ken Blanchard survey of C Suite executives, skill shortages, a top organizational challenge, had increased steadily as an issue since 2003 but declined sharply this year, indicating that more pressing matters are on their minds. For instance, price sensitivity had decreased almost every year since 2003, with the exception of 2007, until this year, when it increased by four percent.

TOP ORGANIZATIONAL CHALLENGES

Ranked by order of importance in 2009

Issue	*2008*	*2009*
Economic challenges	61%	85%
Competitive pressure	63%	64%
Growth, expansion	59%	50%
Culture change	48%	41%
Pricing sensitivity	36%	41%
Innovation	35%	36%
Skill shortages	50%	34%
Global challenges	22%	26%
Government regs	24%	25%
Changing technology	31%	24%
Consolidation	13%	15%
Ethics and social responsibility	13%	13%

Source: Ken Blanchard Companies

Culture change was also added as an issue to this year's list of choices and weighs in a high issue, right behind skill shortages.

TOP MANAGEMENT CHALLENGES

Respondents to the Ken Blanchard study were asked to choose the top five issues they would focus on in 2009 and then in a second question asked which one issue was most important. Creating an engaged workforce, which ranks second, has increased in importance every year since 2003, based on the number of respondents selecting it.

Managing change, an issue that was added in 2008, ranks first, reducing costs ranks third, and developing potential leader ranks fourth. The issue of reducing costs increased more than 10 percent, indicating that respondents are indeed focused on their corporate pocketbooks. The issues of selecting and retaining talent and managing a shrinking talent pool both declined sharply this year, indicating that organizations are more focused on weathering the economic storm rather than on keeping key people. This is surprising when one considers that key talent retention is a source of competitive advantage.

CLOSED LOCATIONS; MORE SECURITY

There is also the closing of work locations during the economic downturn. The CEO makes the decision and others – including security – must carry out the action. Pointed out Harris, "As organizations look at taking work locations out of service because of budget considerations, the process does not translate to a reduction in the security force's workload. In fact, it may actually generate a greater volume in terms of patrols and site checks of those same unoccupied properties."

With all the complex forces in play for CEOs and corporate presidents, it is easy to see the stress fractures. Observed Jordan Johnson, regional security manager, Cushman & Wakefield, "Many CEOs undoubtedly view their organization's security operation as a necessary evil - as an unavoidable source of expense. This can take many forms. Some may view security functions as part of their compliance efforts, while others view them in terms of mitigating risk. In the real estate, property management, and facilities sector, there is an unfortunate tendency to translate everything into a cost per square foot matrix.

"The many different ways in which security is viewed is reflected in the diversity of reporting structures one sees in various industries. Seldom does security as a function report directly to the executive level. The function may report through HR, risk management, legal, facilities, real estate, or environmental health and safety, to name just a few examples. One of the problems with these types of arrangements is that security is an ancillary, rather than a core, concern for these departments.

"The most enlightened CEOs, one hopes, are those who view 'security' in the most expansive terms, and consider all of the various ways an effective security program can contribute to their organization's success."

TOP MANAGEMENT CHALLENGES

Ranked by order of importance in 2009

Issue	*2008*	*2009*
Managing change	55%	59%
Creating an engaged workforce	58%	57%
Reducing costs	38%	52%
Developing potential leaders	53%	50%
Customer loyalty	38%	39%
Selecting and retaining key talent	50%	39%
Mission, vision, values	39%	35%
Aligning culture with strategy	37%	33%
Increasing innovation	29%	31%
Succession planning	27%	26%
Employee flexibility, responsiveness	22%	25%
Managing a virtual workforce	11%	14%
Managing a shrinking talent pool	18%	13%

Source: Ken Blanchard Companies

NEED A SEAT AT THE TABLE

Johnson added, "Top security executives need, more than anything else, a 'seat at the table.' Without a voice at the decision-making level, a security program will be

marginalized. Without strong executive support, it will eventually flounder. Employees who perceive that security is not important to senior management will not view it as important either. In their relationships with CEOs and other top management, security executives need to cultivate trust, openness, and mutual respect. It is critical that they establish themselves as a bona fide content expert in their field of responsibility. Failing to do so will invariably result in a lack of credibility."

He added that defining security purely in terms of deterrence and worst-case scenarios is no longer sufficient - particularly in tough economic times. One can't define value purely through the absence of undesirable activity; one needs to document and demonstrate value.

It's obvious from the Security Magazine survey of what CEOs think that the traditional perception of the security executive is changing and placing more pressure on this security leader to meet CEO expectations.

John Williams, director of security, Prince William Health System, agrees. "Overall, I think to some degree it's changing from necessary expense to value driven. However, I think from the physical security side, depending on your business field, we have a way to go. In some instance the only time security is considered by the C-Suite is when there is a projected expense impact or when an adverse event happens. Again that is more prevalent in some business fields than others. A lot may impact CEO perceptions of security including the value it brings to the business model and how the security administration has positioned within the corporate mindset. Do they try to fly under the corporate radar or do they vie for a seats that the table?"

Echoing other security leaders,Williams thinks trust is a big key as is reasonableness in security recommendations. "Reasonableness goes along with trust and helps demonstrate how the security director sees the overall corporate and business concept and his or her place in it. When it comes to assessments and suggestions that impact the organization, are they high level individuals or silo driven? It's easy to be given an assignment of evaluating the risk associated with a new business line or acquisition, and take the stance that every possible risk associated with it must be mitigated. In a perfect world no one would recommend risk, but in the real world we all take multiple risks everyday."

METRICS TO PROVE TO THE CEO

It's also a matter of metrics.

Added Williams, security leaders "need to identify metrics that are of value to the CEO and the business, then take steps to get those and their recommendations in front of their respective CEOs. The days of trying to fly under the CEO's radar have long gone. Security has to show value and forward thinking to be competitive and integral to their organization.

Concludes Anthony Potter, CHPA-F, CPP, director of public safety, Greater Winston-Salem Market, Novant Health, "Our CEO is probably our single biggest booster, and we have her complete support. She looks at security as a proactive discipline, as I do, and counts on us to keep things from happening." Potter pointed out that "the top security executive must have direct access to the CEO 24/7, regardless of the organization chart and normal reporting relationship."

It's the synergy between the security leader and the CEO.

But the relationship is not always perfect. Added Potter, "I have worked for three CEOs in nearly 20 years in healthcare, and two of them fit the above description. The less said about the third the better. I left his hospital after two years due to ill health. He got sick of me!" SECURITY

CEO REPORT CARD ON SECURITY — 2009

Chief executive officers and presidents rate their security operation in 14 key areas. New in this year's Security Magazine's, respondents placed each of the 14 into three levels – crucial, essential and important as impacting security as well as the business.

Crucial Business Needs Impacting Security

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

Essential Business Needs Impacting Security

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

Important Business Needs Impacting Security

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

Source: A telephone and e-mail survey of 100 CEOs and Presidents of enterprises with a formal security department or operation. All respondents were assured confidentiality.