FORRESTER®

For: Security & Risk Professionals

The CISO's Handbook — Presenting To The Board

by Andrew Rose, October 24, 2013

KEY TAKEAWAYS

Use Analogies To Explain Complicated Technical Concepts

Help the board "visualize" security issues. Often directors and executives in the boardroom are nontechnical people, so it's important to illustrate information security in a more accessible way through common language and general business terms. Security analogies, such as a home robbery, are excellent vehicles to begin conveying complex ideas.

Understand The Business Goal

Recognize why the board wants a CISO in the room. Align the goals of the business with your overall security strategy. Board presentations can often be treated on a case-by-case basis, focusing on the latest security trends, when the reality is that security's role in the business is a far more important issue. Deliver a consistent message.

Be Able To Answer The Classic Boardroom Question

Executive boards are always looking to answer the question "how secure are we?" Break this question down into more tangible terms to help the board understand the fundamentals, such as security posture compared to peers, current security trends, where the gaps are, and how to fill those gaps.

The CISO's Handbook — Presenting To The Board

How To Communicate Effectively At The Highest Level

by Andrew Rose
with Christopher McClean and Thayer Frechette

WHY READ THIS REPORT

Your ability to communicate can mean the difference between success and failure in many aspects of your professional life, and it becomes even more important when trying to get the attention of an executive board. Now that information security has become an essential part of risk management across many organizations, chief information security officers (CISOs) must effectively present their case to boards and c-level executives in order to articulate risk posture, explain strategy, or garner more budget. By understanding the audience, simplifying security issues into nontechnical terms, and mapping out a clear storyline, CISOs can productively position themselves to be key influencers in the boardroom. This report outlines the steps needed to successfully usher information security into the strategic and operational business agenda. This report is an update to the "CISO Handbook: Presenting To The Board" report originally published on April 12, 2010.

Table Of Contents

Notes & Resources

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

Evolve To Become The 2018 CISO Or Face Extinction
September 6, 2013

Develop A Change Plan For Your Security Program
March 26, 2012

How To Market Security To Gain Influence And Secure Budget
January 12, 2011

FAILING TO MEET THE BOARDROOM'S NEEDS CAN BE CAREER LIMITING

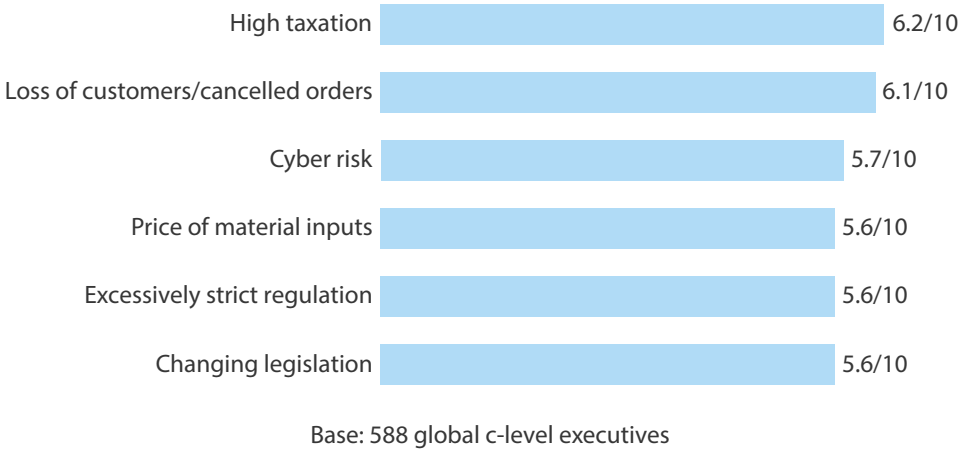
Although it may make many CISOs uncomfortable, the S&R leadership role is clearly evolving away from technical issues toward business responsibilities — and at an accelerating rate.[1] This change requires CISOs to divert attention from the operational aspects of security, such as incident detection, technical configuration, and project consulting, and instead focus on business aspects such as strategy, resource prioritization, and budgetary control. As the expectations placed on CISOs change, so does their environment — the boardroom is becoming the new lair of the security professional, with executive leadership the new bedfellows — but beware, it's a perilous place to reside! CISOs without the skills to respond appropriately all too often find themselves losing influence and seniority.

> "The CISO is like the rider on top of an elephant with a small stick — we are not in a position of power and authority, rather we are in a position of influence. While you must take advantage of every external factor you can — the momentum of the elephant, the direction of the herd, and the landscape around you — and resist when the elephant goes against your desires, ultimately, remember who is really in charge." (CISO in financial services organization)

Information Risk Has Become A Boardroom Priority

CIOs used to report security and information risk issues to the board as part of their IT update. Those days are gone. Executive leaders now see information risk as a key aspect of keeping their organization stable, well regarded, and, ultimately, profitable. A recent study by leading global insurer Lloyds of London, for example, found that cyber risk is now considered one of the top three business risks that companies are facing (see Figure 1).[2] At last, senior executives *care* about information risk management, which means they need to hear the full story directly from the security leader. But this isn't 'job done' for the CISO; this is where the really hard work begins.

Figure 1 Cyber Risks Score High On Board-Level Priorities



Source: Lloyds Risk Index 2013, an Ipsos Mori survey of 588 c-level execs

56343 Source: Forrester Research, Inc.

You Have To Understand Your Audience

For some CISOs, their board-level audience is the executive board, a collection of colleagues all bearing the c-level badge — CIO, COO, and often CEO. For others, their top audience is the board of directors, often made up of executives and nonexecutive directors. For simplicity, consider the two groups in the following way:

- **The executive board members are hands-on managers.** This is a collection of the most senior executives in the organization, with specific areas of responsibility such as finance, marketing, human resources, or production. This group is responsible for developing and implementing the firm's strategy, policy, and program of action and for overseeing the financial affairs of the organization. This group is closer to the day-to-day management of the organization's operations and, as such, you can delight them by addressing their appetite for detail and specificity, including items such as clearly assigned owners and defined timescales.

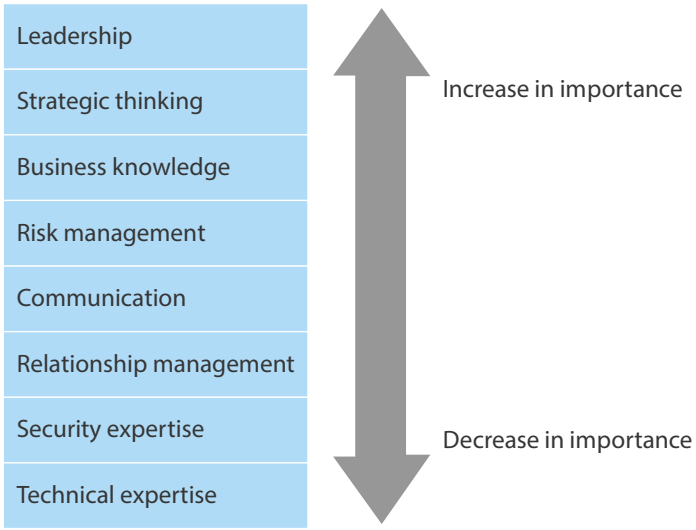
- **The board of directors governs to maximize shareholder value.** This group may be made up of both members of the executive board (see above) and nonexecutive directors. Nonexecutive directors have no internal responsibilities, but they often have specific insight into the organization's industry or have deep experience in disciplines like finance or HR. This board seeks to guide, inform, and oversee the executive team, and it represents the interests of the organization's shareholders. The board of directors acquires significant accountability via regulators and legislation and is strongly incentivized to avoid errors and mistakes; technology is likely to be outside their usual skill set so clear communication, rather than detail, becomes the priority. Provide information that assists them with their focus on governance, profitability, stability, and growth.

Performances Become Sink Or Swim

The first few times a CISO gets direct access to speak to these executive audiences is like walking a tightrope, and if you fail to deliver, it's likely that you will not be invited back. The skills needed to make a real connection are tightly aligned with business focus and not technology; they reflect, and are part of, the evolving role of the CISO (see Figure 2).

Failure to connect with the board is often tantamount to demotion as security is now too important for the executives to ignore. Instead, they hand responsibility for executive communication and reporting to another individual: in some cases the CIO and in others a new, experienced, business-focused person is appointed. In either case, the perspective of S&R leadership starts to lose its association with the CISO, and it's almost impossible to repair that damage.

Figure 2 Business Skills Are Paramount As Security And Technical Skills Wane In Importance



Base: 56 security and risk leaders

Source: Q2 2013 North America/EMEA Role Of The CISO Online Survey

56343 Source: Forrester Research, Inc.

PREPARATION AND CLARITY ARE BASELINE BOARD-LEVEL EXPECTATIONS

CISOs generally receive only a short time window for their board presentations, averaging a single presentation of about 10-15 minutes each quarter. In that time, they need to communicate the key risks and remediation tactics, answer any questions, and get to their desired goals; in an environment where the audience is largely nontechnical, this can be challenging.

"Establishing a relationship with the board is like starting a relationship with a new partner — if you just get to speak to them for 10 minutes every 3 months, then it's going to take a long while to get past anything but a very shallow understanding." (CISO at a financial services organization)

Break Down Difficult Questions Into Manageable Points

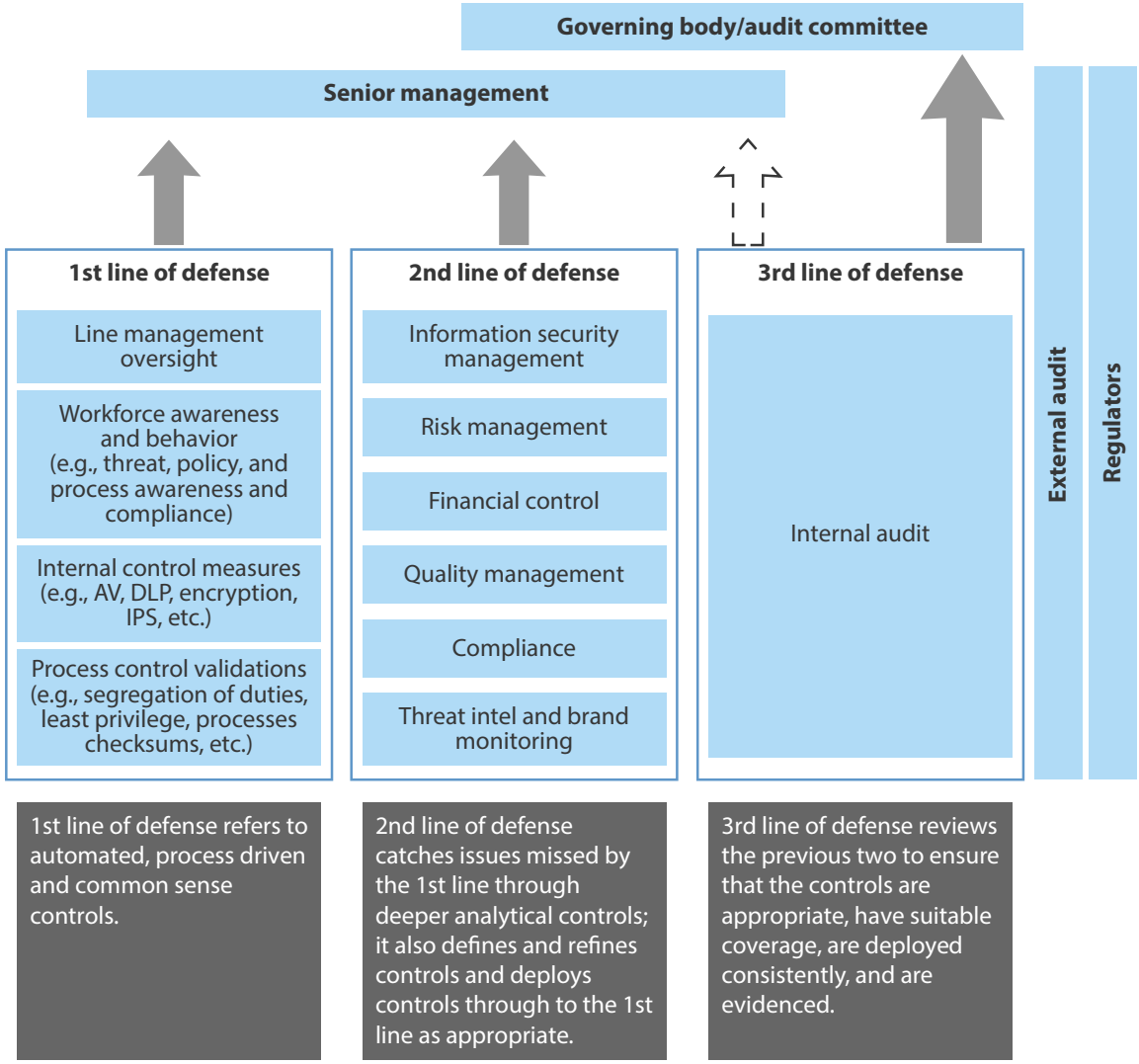
CISOs who present to boards of directors are almost all trying to answer one common question — "how secure are we?" Successful CISOs tend to break down that tricky question into five more manageable questions (see Figure 3). They also pin their answers and current initiatives to clear and consistent models, such as the "three lines of defense" to help their executives navigate the topic without confusion (see Figure 4).

Figure 3 Key Questions For CISOs To Answer

Question	Comment	Key tip
What are the new and emerging trends?	An opportunity to bring new topics into the boardroom, rather than just running through the regular key risk indicators; this is a prime opportunity to preempt any questions and address recent news stories or industry-based incidents.	Add credibility to content by quoting from reliable sources, such as regulators, government bodies, and peer groups. Although a handful of CISOs shied away from inviting representatives of these bodies to speak to their board, those that did seemed to get rewards in the form of priority and buy in.
What is our plan, and our progress against it?	The first of the two key sections of the presentation, this is a recap of the initiatives in place to address current risk issues and give updates on their progress in terms of timescales, budgets, and results.	Simplicity is key. Latch onto the "three lines of defense" model that so many CISOs leverage to describe their control structure in a logical and plain manner. Describe your initiatives within this framework.
How do we compare against peers?	This is a predictable question that you should preempt and design into your presentation. Leverage published benchmarks and industry insight to provide comparison with competing or peer businesses.	Compliance with standards such as ISO27001, PCI, SSAE16, etc., can act as a good touchstone to validate controls and prove progress; they can also be leveraged for marketing purposes.
What is the gap from the ideal?	We all know that reaching a five in a CMMI model is ideal, but often not practical due to reasons of cost and complexity. Show how far you deviate from this 'ideal' status and be clear about justifying that position based on business requirements.	The gap between perfection and reality represents a significant slice of your company's risk appetite. Leverage these gaps to drive prioritization and resource management.
What are the potential consequences of these gaps?	When describing the potential impact related to information risk, ensure that they are laid out in business language. Use terms such as profitability, revenue, and efficiency.	One of the best examples of this practice is an organization that talks about IT risk impacts only in terms of the product that the firm manufactures. (e.g., this information leak equates to 10k barrels of oil).

56343 Source: Forrester Research, Inc.

Figure 4 Forrester's "Three Lines Of Defense" Is A Clear, Concise, And Relatable Model For Boards



56343 Source: Forrester Research, Inc.

Adopt A Clear Style Of Communication To Overcome Boundaries

When standing in front of the board, remember that they are seeking to guide the organization to maximize shareholder returns and avoid costly errors resulting from lack of foresight, oversight, or omission. It's important that you adapt your style to assist the directors in achieving their goal despite any lack of technical insight. There are several ways to accomplish this, including the following:

- **Provide a succinct paper to board members before a meeting so they can be prepared.** Not all CISOs are asked for this, but those that get the opportunity feel it is worth the effort. Giving board members a short summary of key issues ahead of time helps establish a foundation of understanding, allowing the in-person meeting to be more effective and cover more territory. Keep the text short and simple, then include appendices stuffed with data in case the board has additional questions — just make sure you can explain every data point, blindfolded.

- **Tie proposals and suggestions to business imperatives and goals.** Prove that you understand the organization and can separate the "cash cows" from the "dogs," and treat them accordingly.[3] Avoid technical speak; instead, relate risks to business impact, link projects to business objectives, and couch investment in terms of business opportunity and revenue. For example: "The firm recently outlined a commitment to reduce operating cost by 10% and increase revenue by 15%. As a result, we propose to accelerate our virtualization program to reduce hardware spend without compromising functionality, postpone a SIM upgrade to save investment capital in FY2013/14, and leverage that saved resource to enable greater functionality on the sales teams tablets while still managing the associated risk."

- **Analogies and similes are critical; compare security to real life examples they will understand.** Don't talk technical. Think creatively about how you can explain technical issues in more accessible terms — perhaps using physical security analogies (e.g., protecting your home from burglars), insurance policies, or accident avoidance. Analogies were a key differentiator among CISOs most effective at this level, and they used them constantly.[4] One CISO received a piece of golden advice from their board of directors — to craft compelling messages, build each major point on the four pillars of FOAM (facts, observations, anecdotes, and metaphors) rather than on fear, uncertainty, and doubt (FUD), while steering clear of worst case scenario scaremongering which, although potentially successful in the short term, will only undermine executive credibility and support (see Figure 5).[5]

- **Select graphical models to simplify complex data issues.** Find a format that works for your board, perhaps taking ideas and suggestions from your colleagues in enterprise risk, audit, or finance. Create simple visuals based on red-amber-green coding, heat-maps, or trending charts. Avoid wasting precious time by keeping these graphics and metrics consistent for each presentation. Expect every "red" to be questioned.

- **Promote discussion in the boardroom.** Ideally, your deck will not result in stony faces nodding along with your statements. Board members tend to explore issues through discussion, so set out with this aim in mind. Create content, slides, and premeeting papers that move toward an open question and answer session, and support the discussion with facts, data, and expert opinion. Stay aware of timescales, as it's rude of you to overrun, and know the closed questions you'll need to interject with to get the result you desire.

  "I volunteer to go as the last presentation of the day. It means I have to work harder to capture their attention, although using Prezi rather than PowerPoint helps here. As the final presenter, however, I can overrun, accommodate discussion, and get much more time that I usually would." (CISO at a construction firm)

Figure 5 Use FOAM, Not FUD, To Communicate With Board Members

56343 Source: Forrester Research, Inc.

CRAFT A COMPELLING MESSAGE BY FOCUSING ON THE GOAL AND THE CONTENT

A competent CISO will satisfy their board by focusing in on the correct questions and providing suitably clear and succinct answers. S&R leaders who seek to push beyond this level, however, put additional thought, structure, and preparation into their content.

Understanding The Goal Is Vital To A Successful Outcome

Many students wake from terrifying nightmares in which they sit down to take an important exam and found that they have studied the wrong topic. If CISOs wish to avoid similarly sleepless nights, it's important to prepare before strolling into the boardroom, papers in hand, by asking yourself three key questions:

- **Why does the board want my presentation?** Irrespective of whether this is the first meeting with the board, or one of many, consider what the board will be looking to achieve from the meeting. Often, they are seeking assurance that information risk is in hand and that approved projects are progressing without delay. However, many CISO reported that it's commonplace for board members to raise questions related to recent press stories or peer events.

- **What do I want to achieve from this presentation?** Although your main purpose may be to keep the board updated and aware, it's important to consider any other priorities before you step up to speak. Not all CISOs can ad-lib their way to a budget increase, and, for many, a lack of clarity of purpose can lead to discussions that confuse the directors. Being focused on the end goal from the outset enables a much more compelling case to be created through the content.

- **How can I make sure the theme remains consistent?** While the immediate requirement may be to comment on a specific issue, it's important for the CISO to build a consistent theme or message and avoid knee-jerk reactions that may obfuscate any existing road map or strategy. Find your theme by locating the synergies between business objectives and security goals; these may, for example, revolve around protecting customer information, being the trusted vendor, avoiding regulatory censure, or offering new and innovative solutions. Answer the board's immediate questions, but always relate it back to the key themes, as these provide a consistent yardstick for the directors' understanding of your risk tolerance and security strategy.

> "Just going in and just responding to directors questions is like playing golf in the dark; it's certainly playing the game, but the chances of shooting a par are slight, and even if you do, everyone will assume it's luck rather than judgment." (CISO at a legal firm)

Analyze And Refine Your Material To Achieve Maximum Effect

Quite obviously, CISOs need to plan ahead to maximize these opportunities. Consider these key questions as you prepare both the presentation and the supporting document ahead of your next board presentation:

- **How do you want your board to feel after you have finished?** Although the ultimate success of a boardroom presentation is measured on whether you reach a successful outcome, one CISO took this to the next level, spending time considering how she wanted the board members to feel after she left the room. Eventually deciding upon words such as "aware" and "assured," this gave an effective mission statement to the board interactions that enabled the messages to be crafted to ensure a successful delivery every time.

- **What is the storyline that leads to the right outcome?** Stories are one of the most effective ways of communicating, and they can be used as powerful tools enabling points to be made without resorting to technical detail. Remember the three-stage story process — find a hero the listeners can relate to, define the problem, and then resolve the issue with action. Take advantage of press stories to walk the directors through key scenarios; invite external guests from industry groups or government to provide perspective and insight; use video or quotes from customers and peers to make your facts speak for themselves. Directors will take compelling stories with them when they leave the room — that rarely happens with charts and technical documents.

- **Is there another side to the tale?** It is critical to present the board with all relevant information when key decisions are on the line; holding back data that undermines your point is an ethical faux pas that is likely to be career limiting if it gets out. Ensure that your deck creates a balanced perspective of the situation at hand. Feel free to recommend a course of action — that's what you are paid for — but don't stack the deck in your favor.

- **What good news can you include?** It's easy for the CISO to get a reputation as a doom-monger, always highlighting worst-case scenarios, few of which ever come to pass. In some cases, it's important to explain how bad things might get, but doing this too often is damaging to your credibility. CISOs need to balance the content to try and communicate success stories and opportunities for innovation rather than only being consulted when there is a crisis at hand.

- **Are there opportunities to socialize the content before the presentation?** Where possible, it's always best to talk to an audience that already supports your perspectives or proposals. Although access to nonexecutive board members is a rarity, you can consult key executives before meetings, and for significant issues this is a fantastic idea. Work with powerful peers in functions such as compliance, legal, and audit by tying your message to theirs or getting them to restate and support your message. Ensure that you avoid last minute surprises by having as many people at the table already on your side.[6]

  "Don't be the sole harbinger of doom and despair. Socialize your message and your plans so, when you stand up in front of the directors, you are just one voice in a choir, all singing together and calling for action." (CISO in a financial services organization)

WHAT IT MEANS

THIS IS YOUR SHOWCASE — BREAK A LEG!

A security and risk leader who aspires to reach, or stay at, a position of corporate executive relevance has to recognize that the next few years will stretch and challenge them. You'll need to lay the foundation of new skills and relationships upon which to build your success. The sponsors you gather now will support your career for many years to come, so it's vital to maximize the quality of those interactions. Nowhere is this more important than the boardroom — the audience here hold the keys to your long-term success, but are also the harshest critics. Prepare, practice, and know the whole script backward and forward, and you are sure to be a star.

ENDNOTES

[1] As the role of technology leadership in the enterprise becomes more about managing third parties, battling complexity, controlling costs, and aligning with business strategy, the role of the CISO is shifting to one of a business manager who specializes in change management and process oversight. CISOs will need to realign their priorities and build new skills if they want to remain in their jobs. For more information, please see the September 6, 2013, "Evolve To Become The 2018 CISO Or Face Extinction" report.

[2] The findings from the three Lloyd's Risk Indices show an interesting pattern in terms of risk management. Cyber risk has become a top three concern, but businesses readiness to address these risks has remained largely complacent. For more information, please refer to the survey. Source: "Lloyd's Risk Index 2013," Ipsos Mori survey for Lloyds, 2013 (http://www.lloyds.com/~/media/Files/News%20and%20Insight/Risk%20Insight/Risk%20Index%202013/Report/Lloyds%20Risk%20Index%202013report100713.pdf).

[3] The Boston Consulting Group's matrix can help you separate the "cash cows" and the "dogs." The matrix is designed to determine the overall prospects of various business units. For more information, refer to the related article. Source: Andrea Ovans, "Vision Statement: The Charts That Changed The World," Harvard Business Review, December 2011 (http://hbr.org/2011/12/the-charts-that-changed-the-world/ar/1).

[4] A number of S&R leaders have started to collaborate, collecting together useful and effective analogies that they have used to convey key messages. Review these analogies to give you fresh ideas, and submit your own for the good of the community. Source: The Analogies Project (http://www.theanalogiesproject.org).

[5] The terms metaphor and simile describe the linguistic means that we use to draw an analogy (as most analogies use either metaphors or similes to achieve their purpose). An analogy is a general term to refer to the use of familiar examples in order to explain something that is generally unfamiliar.

[6] For more information on how to help identify, align with, and influence critical stakeholders whose support they'll need to embark on change programs, see the March 26, 2012, "Develop A Change Plan For Your Security Program" report.

FORRESTER®

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals