Five Tips for Security and Risk Leaders When Communicating With Business Stakeholders

Published: 29 June 2015

Analyst(s): Jeffrey Wheatman

While security leaders have improved their communication with business stakeholders, a gap still exists between what is said and what the business hears. The lack of communication skills continues to cost security leaders a voice in strategic planning and a seat at the executive table.

Key Challenges

- Communication difficulties represent one of the major reasons for the failure of security and risk management activities, and for the marginalization of security and risk management organizations within enterprises.

- Security and risk management professionals continue to struggle with translating risks into business language, and clearly articulating IT and security risks in terms the business understands and cares about. They speak a different language from business leaders — and they shouldn’t expect business leaders to bridge this communication gap.

- Security and risk management professionals not only communicate differently from business leaders, but also communicate about different issues — issues that are commonly not of interest to business stakeholders.

- For security leaders to improve the effectiveness of security and risk management programs, they must clearly articulate the connection between IT risks and business impact.

Recommendations

- Recruit security and risk management program leaders with proven business skills. The CISO role is largely a business leadership role, and organizations looking to hire CISOs should focus on both soft skills and hard skills. Seek individuals with broad business, communication and leadership skills and experience, and those who can address the needs of the business.

- Encourage and motivate security and risk management personnel to acquire the skills needed to communicate effectively with business peers. This may mean anything from studying business writing or communication to taking internal training to learning about how the enterprise or a specific business unit works.
Seek out and cultivate sympathetic stakeholders across the enterprise who can help you refine and communicate the security and risk management message. Use their expertise to identify accessible early wins that can demonstrate the business value of security and risk management efforts to a larger audience.

Introduction

CISOs and other security and risk management leaders continue to struggle to be treated as equals by other C-level executives. A recent survey by ThreatTrack Security\(^1\) indicates that CEOs and other C-level executives don’t have confidence in the leadership skills of the CISOs in their organizations — for example, the survey notes that 61% of executives do not believe their CISO would be successful in a leadership role outside of information security.

Gartner client inquiries make it clear that one of the most serious problems facing security and risk management professionals — and one that is undermining their credibility — is their inability to communicate effectively with senior executives, line-of-business managers and other key business decision makers. CISOs and others with security and risk responsibilities find it extremely difficult to articulate their agendas; demonstrate the value of their programs, processes and controls; indicate that they understand the key risks of their business “clients”; and — crucially — to justify the expenditures on their activities. These communication problems have adverse effects that flow in the opposite direction as well, with security and risk management efforts that fail to meet the needs of the business. The result is a vicious cycle, in which poor communication results in inefficiencies and failures, which, in turn, diminish the perceived value of the enterprise’s security and risk management initiatives.

Not only do business leaders mistrust security leaders, but also security leaders themselves don’t believe they are effective communicators. An audience poll conducted at Gartner’s 21st annual Security and Risk Management Summit indicated that almost 30% of respondents rate themselves as less than somewhat effective at communicating to their stakeholders, and only 11% stated that they were very effective at communicating (see Figure 1).
Gartner has identified five areas for improvement in CISO communication that will bolster their reputation and help them to be perceived as more business-aligned, and will start to change the perception that the CISO is just another technical resource who doesn’t understand the business. CISOs and other security leaders should strive to improve interactions and learn to more effectively communicate with the business on the business’s terms. There are no simple solutions, but an ongoing effort to improve communication will deliver clear, recognizable benefits. There are five key reasons security professionals can’t communicate effectively and productively with the business.

Analysis

Tip No. 1: Learn to Speak the Language of the Business; Don’t Expect Business People to Learn the "Secret Language" of Security

A large number of security personnel tend to come from technology backgrounds. A typical career path for a security professional has been to start out as an administrator, engineer or analyst, and then to progress through a variety of technical roles. It is natural for these individuals to think and speak in technical jargon.

Moreover, it is a basic human tendency for people who are under stress — and security and risk management professionals are almost, by definition, under constant stress — to fall back into their
comfort zones in terms of what they talk about and how they talk about it. Thus, they communicate about security and risk management issues from a technical and tactical perspective, and in technical and tactical terms. In essence, they talk about threats, when the only thing that interests the business is the risk resulting from those threats.

What to Do About the Problem

■ Practice your approach, recording yourself on video and watching and listening to your presentation. If you were a business stakeholder, would you care about what you are hearing? Does it interest you or engage you? If not, then you need to work on your presentation skills.

■ Honestly evaluate your own presentation. This may be the most difficult activity to undertake with regard to closing the gap in the communication channels, but it also may be the most important. Try to independently evaluate the content and delivery of the message. Think about how your audience might understand what you're saying. Consider practicing with peers, and get feedback from them as part of the preparation process.

■ Vet your message with a nontechnical audience and solicit honest feedback.

■ Pay close attention to your audience. If your listeners look bored — if they're glancing at their computers or their mobile phones, for example — they probably are.

■ Leverage terminology and phrases used in business strategy and communication in your talk track. Mirroring the business’s language verbatim ensures that the business believes you are paying attention to what is important to them.

Tip No. 2: Seek Out Business and Communication Training and Education

Security and risk management professionals have seldom been trained in how to communicate in a business setting. Sometimes, the problem isn’t what you say, but how you say it. If the presentation is poor, it will be difficult to get your point across, even if the message is strong. Few security and risk management professionals have received training in how to speak to the business in language the business understands, or regarding issues that matter to the business. Gartner’s advice to enterprises has been to recruit security and risk management leaders with business backgrounds and experience, rather than strictly technical expertise. For those organizations looking to promote from within, these leaders should be trained in communication, presentation and facilitation skills.

It is important for security and risk management personnel to move beyond the stereotype of the introverted, uncommunicative “tech geek,” and develop individuals who are comfortable discussing IT risk and security issues with senior business leaders in terms that those leaders understand and care about. In many respects, this is fundamentally a question of moving away from technical jargon and narrow technical concerns.

Another critical issue is learning to avoid overloading business leaders with excessive detail. A 50-page document or a 50-slide PowerPoint presentation is likely to have the opposite effect of what is intended, and may cause the intended audience look at only the opening page or slide — or to ignore the deliverable entirely. Be prepared to answer questions in detail, but don’t base your presentation on the recitation of highly technical details.
What to Do About the Problem

- Recognize that meetings with business managers are not only inevitable, but also desirable, and prepare appropriately for them. As the old saying goes, "You don't get a second chance to make a first impression," and you can't expect to improvise successfully.

- Take a class in business writing, presenting or related skills. Find out whether an enterprise training program or budget is available, and learn business-focused skills (instead of, for example, getting another security certification).

- Consider a postgraduate business course (such as an MBA or other business education certification).

- Leverage the enterprise's available communication tools. If a standard document or presentation template is available, then use it instead of trying to create your own. Be careful about getting overly dependent on the "bells and whistles" that presentation software offers — say "no" to clip art and images that don't contribute to the message.

- Create a taxonomy document, and populate it with appropriate business terminology. Technical jargon, buzzwords and other specialized terminology can sometimes be helpful, but they should be used sparingly and in the appropriate content.

Tip No. 3: Recognize That Business Leaders Are Extremely Busy; Respect Their Time by Being Concise and Clear

The simple reality is that business leaders are occupied with issues that do not bear directly on security and risk management, and the higher the level those leaders are — and it is, of course, the higher-level leaders who the security professional needs to reach — the busier they are. The business leader's primary concern is to deliver on the goals of the business, so it is always difficult to find time in their schedules. When a security professional does manage to gain the business leader's attention and fails to use that opportunity effectively to demonstrate the value of current or proposed activities, it will be even more difficult to get on that business leader's schedule next time. Moreover, and even more crucially, this disengagement means that the business leader is not involved in the security and risk management decision-making and governance processes, and is far less likely to be accountable and accept responsibility for residual risk.

Show directly how what you are doing contributes to the business outcome that your business peers have to achieve. Show how a goal will be met. Demonstrate how you are making a key business process more resilient. Discuss how you are reducing their costs by improving efficiency or reducing their risk.

What to Do About the Problem

- Connect your message to an identified business goal or existing project, and get that in front of the audience as quickly as you can. Make sure you understand and can articulate the organizations mission and vision. (A recent audience poll of 400 security leaders at Gartner's 21st annual Security and Risk Management Summit indicated that less than 10% of those present knew what the vision and mission of their organization were.)
Structure your business cases and reports so that the most critical information is upfront. Make certain that your key points aren’t buried. You can always include supporting information (which is especially important if you won’t be presenting your points in person).

When speaking, be succinct, but not brisk. Tell your audience why they should care about the subject, and make it clear that you’ll be happy to give them further details at a convenient time. Pay careful attention to how much time you spend talking versus listening. If you talk too much, then you may fall in love with your own words.

Don’t make assumptions about what the audience knows or understands. Be ready to explain or support the message, but don’t tell them everything you know all at once.

Tip No. 4: Recognize That Business Stakeholders Will Not Always Express Their Concerns in Terms That Security and Risk Professionals Understand

Security professionals are not the only ones who have difficulty communicating effectively. Business leaders also struggle to articulate their concerns. Nonetheless, it is the security professionals’ responsibility to overcome this problem. Compliance issues provide a classic example: For the business, compliance is simply a set of rules to be followed, and, if the rules are followed, the business considers itself to be safe and secure (for example, with Payment Card Industry [PCI] standards).

However, from a security and risk management perspective, the issue is far larger. The business may recognize that a failure in PCI compliance will result in a downgrading of the enterprise’s PCI status, which could cost millions of dollars in card processing fees. The security professional recognizes that the enterprise can be PCI-compliant and still suffer a data breach (for example, Target and Home Depot both had recently passed PCI audits before their respective breaches). Business leaders do not understand that they need to take a broad-scope approach to protecting regulated or otherwise-sensitive data, of which PCI is just one component. The security professional recognizes that the same processes used for PCI compliance can be used in overall data protection and governance, protecting the enterprise against financial loss, reputational damage and regulatory scrutiny — and potentially saving significant amounts of money. For all these reasons, security professionals must be prepared to ask business leaders business-oriented questions, and to receive and correctly interpret responses and questions from business leaders that may be couched in business-oriented language.

What to Do About the Problem

- Understand your audience. Senior managers and business unit leaders care about different issues from line managers or team leads, and business leaders will hear different messages from their peers in IT.

- Make sure you understand the goals and initiatives of the business units. Business leaders don’t expect you to be an expert in their fields, but you can’t help them achieve their goals in a risk-resilient way if you don’t know what their goals are.

- Recognize that this is your problem to solve. The business can’t be expected to learn your language. Once you’re able to get business leaders’ attention and demonstrate your support of
their goals, it will be easier to engage them in a dialogue in which you can work toward gaining consensus as to what the actual risks are. Create mechanisms to help nonspecialists conceptualize and rank their needs for confidentiality, integrity and availability protection.

Tip No. 5: Work With the Business to Understand Its Appetite for Risk; Even Better, Work With the CRO to Understand — or Define — Risk Tolerance as a Policy Element

Business leaders often struggle with the concepts around information security risk — they know it when they see it, but are hard-pressed to define it or explain the things they are concerned about. If business leaders cannot clearly identify or articulate their degree of willingness to accept information security risk, then security and risk management professionals cannot be expected to put effective and appropriate security controls in place. It is extremely difficult — if not impossible — to quantify information security risk, and risk definitions and acceptance vary widely from industry to industry, from enterprise to enterprise, from business unit to business unit and from individual to individual. The resulting confusion can be highly damaging, and not only because it may lead to inadequate security controls for the real-world risk the enterprise faces. The opposite may also be true, with excessive controls that are extremely onerous and burdensome for the enterprise’s necessary business processes. (This problem is sometimes expressed, colloquially but accurately, as “putting a $10 fence around a $5 horse.”)

For this reason, one of the most important steps that security and risk management professionals can take is to conduct a comprehensive assessment of not only the enterprise’s risk profile, but also its current state of information security risk maturity (see “ITScore for Risk Management” [Note: This document has been archived; some of its content may not reflect current conditions.] and “ITScore for Information Security”). The maturity assessment process is particularly crucial, because Gartner research has shown clearly that enterprises that are more mature from an overall risk management perspective are also more effective at discussing and dealing with risk-related issues in specific domains. Improvements in risk maturity will result in improved security and risk communication, which will, in turn, result in improved risk management — helping to turn a vicious cycle into a virtuous one.

What to Do About the Problem

- Leverage existing models or methodologies for communication, assessment and management of risk. Numerous frameworks and methodologies are commonly accepted in enterprises. Adopting the terminology that is already used in business risk discussions will enable security leaders to focus on the message and not the nomenclature.

- Develop a lexicon of risks that includes definitions. Develop and socialize the concepts around the valuation of assets, as well as the impact and likelihood of risks.

- Avoid using quantitative risk assessments that are difficult to substantiate. Rather, use scenarios or stories to demonstrate and personalize the impact and likelihood of risk. Complicated graphics and discussions of probabilities don’t always resonate. Laying out a story of what could happen is far more interesting and is more closely related to reality.
Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Survey Analysis: CISOs Should Seek Female Security and Risk Management Professionals for Their Teams"

"Two Simple Techniques to Facilitate Business Alignment"

"Eight Practical Tips to Link Risk and Security to Corporate Performance"

"Digital Business Forever Changes How Risk and Security Deliver Value"

Evidence
