Critical Success Factors for Cybersecurity Leaders

Not Just Technical Competence

By Richard Klimoski

The chief information security officer (CISO) role is evolving. Given the dynamic and evolving nature of cyber threats, the key to being effective as a senior cyber leader is to build and maintain credibility. Both the potential cyber leader and his or her supporting organization have a role to play in building and maintain credibility in the eyes of key stakeholders. In this article I offer several suggestions on how to go about doing this.

According to GlaxoSmithKline CISO Robert Coles, "The primary job of the CISO is to convince key stakeholders that threats to cybersecurity should not be seen somehow as representing an acceptable risk." While most managers have had to come to grips with enterprise risk in the areas of finance, operations or even human resources, the cyber risk domain represents uncharted territory. The reality is that the scope of threats to the enterprise posed by such things as denial of service, theft of intellectual property, identity theft and loss of customer can be enormous.

Traditionally the responsibility for enterprise risk management falls to the "chiefs" who make up the senior leadership team of the company (e.g. CEO, COO,

CFO, CTO, and CIO). In a publically traded organization, one might expect that the board of directors also have a role to play. But if every member of a leadership team is responsible when it comes to cybersecurity, then who is really in charge? Based on the many reports of cybersecurity breaches and the huge loss estimates reported every day in the popular press, it appears that real leadership in this domain has been lacking.

The CISO Role Depends on Credibility

The CISO represents a new role as potential member of the top management team. In general, he or she holds deep knowledge of the risk potential of information technology and has the business acumen necessary for a deep appreciation of business processes that need to be installed and maintained to be successful as a firm.

Kathleen Richards, editor of *Information Security Magazine* points out that the CISO position is currently found in firms with 1000 or more employees. In these larger firms the CISO has a "dotted line" relationship with key executives in IT operations, data center management, corporate compliance, and enterprise risk and privacy officers. She quotes Bruce Brody, a past CISO in several government agencies and now the chief cybersecurity strategist at Cubic Corporation, "*…the person who would be the CISO needs to have the ability to communicate across the divide of senior management and engineering [but] be equally comfortable in the coat-and-tie boardroom as in the Hawaiian shirt-and-jeans back office and IT department*" (Richards, 2014). Richards also reports that the market researcher Gartner recommends that companies with as few as 150 employees consider hiring one.

CIO and CISO: BFFs or Inevitably At Odds

The issue of the most appropriate reporting relationships for this new position has received a great deal of attention. Much of this has focused on how to link the roles of the CISO to the CEO and chief information officer (CIO) and whether the CISO should "have a chair at the board table." The emerging thought on this is that the CISO and CIO really have different mandates. Bruce Brody, CISO at PricewaterhouseCoopers puts it this way: The job of the CIO is "power, ping, and pipe," while the role of the CISO is to "defend, react respond, and recover."

Clearly they must work closely together and separating the former from being a member of the IT operation may work against this. However, Greg Shumard, who served for 11 years at CIGNA and who is currently an advisor at Tenable Network Security, makes it clear that when it comes to the inevitable disagreements regarding investments in such things as IT technology, cybersecurity threat mitigation or data governance policy, the CISO must have "an escalation path." He argues for ensuring that that there is the "*power of the position to escalate disagreements to the appropriate CEO or Board position for review consistent with risk assumption guidelines*" (TechTarget, 2013).

John Chambers, CEO of Cisco Systems, supports this point of view. Shumard also notes that when the CIO and CISO go together before Boards together their request for resources to deal with cyber threats or for policy support would be like a "one-two punch" and thus be seen as much more credible (CIO Journal, 2015). All this said a recent survey of where the CISO "fits in" to the leadership structure found that 47 percent reported to their CEO, 45 percent to the CIO, and 4 percent to the chief compliance officer. Only 2 percent report to the COO or CFO (ThreatTrack Security, 2014).

How CISOs Add Value

The details of the CISO role are only now being fleshed out. One way to characterize the responsibilities for this new C-level position can be found in survey results by the Ponemon Institute asking a sample of 113 CISOs what they consider the "best day on the job" (reported in Richards, 2014). According to respondents, when it comes to dealing with cyber threat-related issues a best day would involve having:

- Identified and system vulnerability (19 percent)
- Stopped a cyber crime (32 percent)
- Solved a cyber crime (33 percent)
- "Protected" a colleague from risk (5 percent)
- Secured funding (3 percent)
- Persuaded management (3 percent)
- Educated management and the Board (3 percent)
- Received recognition (2 percent)

While the role or position of CISO is still being shaped, a few things are becoming clear regarding practices that he or she might employ in order to be effective.

A recent report published by the IBM Center for Applied Insights captured several ways the CISO can add value to the firm:

- Contribute to the development of a strong strategy around enterprise risk management with special attention to cyber threats
- Promote a comprehensive risk management platform
- Establish effective relationships with operational managers by understanding their needs, issues and concerns
- Exhibit the practice of extensive, continuous and effective communications around risk threats and risk management opportunities

The report profiled several companies (Starwood Hotels & Resorts Worldwide, BB&T, and Bharti Airtel Limited) and their respective CISOs (Shamia Naidoo, Ken Kirby, Felix Mohan) as illustration of these contributions.

Credibility as a Critical Success Factor

The importance of winning influence with other executives is clearly in the critical path to a CISO's success. Senior cyber leaders require organizational leadership and executive management support to be able to effectively carry out their responsibilities. Joseph Granneman CEO of Search Security.com believes that this can only happen if the CISO exhibits skill listening to executives' needs and matching them to information security objectives. This requires extensive CISO

outreach, with the intent to build credibility and a capacity to obtain buy in when it comes to recognizing and sharing information about potential cyber threats or garnering the resources to address them. Kirby of BB&T puts it this way:

> "…I spend a lot of time building trust with the C-suite and the board. I am constantly reaching out to the individual members of the board and executive management team, developing personal relations. Different members of the C-suite have different worries that I have to address" (IBM 2013, pg. 7).

When drilling down on CISO credibility, at least four themes can be identified:

- **The CISO must be seen as trustworthy.** He or she must be known for integrity and genuinely concerned for the wellbeing and success of others. The CISO must take advantage of every opportunity to do the things that will build and promote integrity. Being trustworthy also implies that the CISO is seen as competent and can deliver on promises made. Because the nature of cyber threats and the means to tackle them are constantly evolving, this means the CISO must be in a continuous learning mode, always expanding their own competence.
- **CISO credibility is enhanced by confidence.** Exhibiting the right level of confidence at the right time is a skill in and of itself. As the saying goes, "confidence without competence is arrogance." It is also clear that because of the evolving nature of cybersecurity threats and the uncertainty this implies stakeholders need to feel that the CISO is reasonably confident in his or her recommendations.
- **It helps to have a track record.** While seemingly obvious, credibility is increased when the CISO can point to cases where he or she "got it right," including such things as assessment of cyber risks, the strategy put in place, or the approach to team work used to implement risk reduction practices.
- **You need an extensive network.** A major feature of credibility is having and using an extensive personal and professional network of individuals that can support the CISO, especially in high stakes situations like gaining support for a comprehensive cybersecurity strategy, obtaining funds for security-related initiatives, or for ensuring compliance to cybersecurity policy. In short, the CISO needs to have a large reservoir of "social capital" from which to draw on when needed. This social network often provides the knowledge and insights required to keep abreast with developments in the cybersecurity arena, especially in light of the understandable reluctance of specialists to publically report on threats, instances of cyber crime, or to share best practices or technical advances aimed at threat mitigation because they may reveal past failures to do so. To keep abreast of such things the CISO must be "well-connected."

Building the CISO Talent Pipeline

Character, competence, a performance record, and social capital are the keys to securing the right talent.

Character

Character can be thought of as a reflection of personal attributes especially an individual's moral or ethical identity. "Good character" is often associated with being seen as trustworthy. As a leader do you project such things as integrity, behavioral consistency and a concern for others? Do you demonstrate capacity for reflection and perspective taking or for using power or exerting influence in a principled manner? Many believe that character is reflected in the willingness to exhibit courage, to take a risk "primarily motivated to bring about a noble, good or worthy end, despite the presence of emotion or fear" (Amos & Klimoski, 2014). As a senior leader courage may be demonstrated by thoughtful but respectful dissent or the willingness to "speak truth to power". Character provides the foundation for credibility. It should be "top of mind" for those seeking to be part of or those responsible for building out the cybersecurity leader pipeline.

Competence

Domain knowledge is absolutely necessary for credibility, but to be successful in a senior cybersecurity leadership role the challenge is recognize that there is no simple answer as to which of the many areas of knowledge, skills or competence identified by the National Initiative for Cybersecurity Careers and Studies (NICCS, 2015) are likely to matter most. In all likelihood whether stakeholders will be impressed by such things as "knowledge of applicable laws" or "the capacity to fashion disaster of recovery or continuity of operations plans" will depend a great deal on the business context and the kind of assets to be protected, the strategy of the firm, or the recent history of the company when it comes to cyber threats. The competencies needed for perceived credibility will also depend on just where the CISO fits into the structure of the organization.

Cyber threats and mitigation approach can vary with the industry sector. Thus those involved in senior cyber leadership roles in regulated sectors like finance or banking may need a different talent profile than those in sectors like critical infrastructure or the selling of consumer products or services. This means that those aspiring to be a CISO, or a firm desiring to grow the talent pipeline for this position, need to appreciate what talent profile is called for and how best to ensure credibility based on competency.

There is a widely shared perception that those who play a CISO role are all too frequently over-specialized. In one survey of executives, 68 percent of respondents felt that most CISO's did not possess a sufficiently broad awareness of organizational objectives and business needs to be seen as credible (ThreatTrack Security, 2014). When members of the senior leadership team "grade" their CISOs as "excellent," it is largely because they have demonstrated value beyond information security by aligning cybersecurity with business goals.

According to Steve Katz, one of the very first CISO's in the field and currently an executive advisor at Deloitte, cybersecurity professionals "*must also look at themselves as part of the entire business model, not just security, and to be able to fully*

understand the business they are in, the problems and business risks that a certain product or service is going to address and how to integrate security into business and business into security" (Spidalieri & Kern, 2014, pg. 6). In the end, the competencies needed for credibility may be not that different than those that promote respect for any senior organizational leader: CISOs must enable the organization to succeed and to reach its strategic objectives (ThreatTrack Security, 2014).

Even if one has the skill set to succeed as a CISO, the bigger challenge to credibility can be demonstrating these skills. Having a formal degree (e.g., an M.B.A. or a Master's of Science in secure information systems) or being able to show that you have key certifications (e.g., CPP, CISSP, CISM) can help. Particular certifications may be required for mobility in organizations that must meet certain compliance requirements, and may even promote added credibility in the minds of "techies" who must be managed. Specific certifications have also been found to be associated with higher average compensation (Stewart, 2013). Demonstrating a propensity for continuous professional education can help build or maintain credibility.

> When members of the senior leadership team "grade" their CISOs as "excellent," it is largely because they have demonstrated value beyond information security by aligning cybersecurity with business goals.

Technical competence alone is not enough when it comes to being seriously considered for an open CISO position (Kern & Peifer, 2015). In fact two other approaches might be far more important:

Performance Record

A traditional way to establish credibility is to point to a succession of accomplishments in previous positions of increasing responsibility. This can also present challenges, as observed by Mark Aiello, president of cybersecurity staffing firm, Cyber360 Solutions, because there is no actual path to the CISO job. As a result most CISOs are hired from outside the company: "*Most companies want to hire a CISO who is already a CISO somewhere else*" (Holmes, 2015). Aiello also points out that most CISO's start their career and have a record of accomplishments in a technical area associated with information technology; it also helps to have performed well in senior positions associated with information security, as long as this experience is within the appropriate industry sector. A career trajectory involving policy or compliance positions can also help. The key is to proactively develop a portfolio of cybersecurity knowledge and experience.

Social Capital

It is generally recognized that building and using social capital is among the best ways to achieve credibility. Social capital reflects the value of connections between people. It is usually a function of the set of relationships (your personal network) that you build and maintain in your efforts to get things done, to get ahead, and to develop personally and professionally.

Your personal network affects many things including your access to information, resources, referrals and opportunities. It contributes to your ability to mobilize people and to exert influence when needed. It implies your potential capacity to add value to others (Edelenbos & Klijn; 2007). It certainly affects your reputation. Given the demands of cybersecurity leadership leveraging your personal network can also be an efficient way to maintain technical competence in the face of technical developments unfolding so rapidly so as to preclude traditional approaches maintaining currency (e.g. formal training).

New threats to information and information technology appear daily. As soon as a solution is engineered, inevitably new vulnerabilities are uncovered. In this regard, the CISO must be (and be seen as) a key player in what has been described as a "knowledge management system" (Zarraga & Bonache, 2003). In such a system the goal is to ensure that valid and timely information is acquired, learning gets absorbed by the firm and is transferred to the appropriate parties in an exceptionally fast manner. Being well connected would be an asset here.

In the case of cybersecurity, this usually means assembling and using information about potential or current threats, about probable harm to company assets and, importantly, on how to best deal with what may be a series of cascading events that might turn into a crisis. Timely warning, quick analysis and appropriate responding are at a premium. Having a robust social and professional network and extensive social capital creates what some authors have called "the ability to surge". It allows the CISO and his or her company to bring the best expertise whether found within or outside the firm to bear on threats, problems or opportunities (Cross, Cowen, Vertucci & Thomas, 2009).

Building Credibility as a "Joint Venture"

If credibility plays such a key role in promoting the success of a potential senior leader in the cybersecurity space, it seems that both the rising executive in this sector and his or her firm have a joint responsibility to develop this strategic capability. Many of the suggestions for building credibility being offered above require personal and professional investment on the part of the executive. It's also obvious that the firm can do much to accelerate the individual's credibility growth trajectory.

HR departments can take the lead, applying practices often appropriate for high-potential individuals, such as subsidizing professional education or helping find stretch assignments to build a track record. They can help cybersecurity professionals develop "network connectedness," bridging silos and building trust (e.g., placing the individu-

al in a senior strategic staff role as a temporary assignment).

HR leaders can also explore ties with other firms that face similar cyber risks and threats, such as helping the individual fill a representational role in a trade organization. This permits them to connect with technical experts operating on the leading edge of information technology or with thought leaders who are shaping public policy, and perhaps encourage them to take on leadership positions in professional or scientific societies.

PricewaterhouseCoopers, for example, offers an innovative leadership development program focuses explicitly on building networks. This five-month program involves in depth discussions with business leaders both within and outside the company (Ibarra and Hunter, 2006). Through such connectedness it is more likely that threat profiles facing the company and appropriate response can be more completely understood and cyber risk better managed. This would certainly add credibility of any person aspiring to be the next CISO.

Richard Klimoski, Ph.D., is professor of psychology and management and area chair in the School of Business at George Mason University. He can be reached at rklimosk@gmu.edu.

References

Amos, B & Klimoski, R.J. (2014) Courage: Making teamwork work well. *Group and Organizational Management*, 39, 110–138.

Cross, R., Cowen, A, Vertucci, L. & Thomas, R.J. (2009). How effective leaders drive results through networks. *Organizational Dynamics*, 38, 2, 93–105.

Edelenbos, J., & Klijn, E.-H. (2007). Trust in complex decision-making networks: A theoretical and empirical exploration. *Administration and Society*, 39, 25–50.

Granneman, J. (2013). What attributes is necessary to have success in the CISO role? (Found at www.searchsecurity.techtarget.com; 5 December, 2013).

Holmes, D. (2015) How the skills shortage is killing defense in depth. *InformationWeek* (found at www.darkreading.com/operations; 1 January, 2015).

IBM (2013). A new standard for security leaders: Insights form the 2013 BM chief information security officer assessment. IBM Center for Applied Insights. (Found at IBM.com/ibmcai/ciso; 30 September 2015).

Ibarra, H. & Hunter, M. (2007) How leaders create and use networks. *Harvard Business Review*, January.

Kern, S & Peifer, K. Senior Cyber Leadership: Why a technically competent workforce is not enough. The Cyber Security Forum Initiative. (Found at www.scfi.us; 9 September, 2015).

National Initiative for Cybersecurity Careers and Studies (2015). U.S. Department of Holland Security. (Found at www.niccs.us-cert.gov; 24 August, 2015).

Richards, K. (2014) Has the CISO role changed under the spotlight? *Information Security Magazine* (Found at www.infosccuritymag.com; 15 September, 2015).

Shumard, C. (2013) Opinion: Definition of the role of the CISO: still a work in progress. (Found at www.searchsecurity.techtarget.com; 16 July, 2013).

Spidalieri, F. & Kern, s. (2014) Professionalizing cybersecurity. Pell center for International Relations and Public Policy. (Found at www.salve.edu/pellcenter; 30 August, 2015).

Steward, J.M (2013) Global Knowledge Training, LLC (Found at www.globalknowledge.com; 20 August, 2015).

ThreatTrack Security (2014). No respect: Chief information security officers misunderstood and underappreciated by their C-level peers. (Found at www.threattracksecurity.com; 15 September 2015).

Zarraga, C. & Bonache, J. (2003). Assessing the team environment for information sharing: An empirical analysis. *International Journal of Human Resource Management.* 14 (7) 1227–1245.