Global Information Assurance Certification Paper

Selling Your Information Security Strategy

GIAC (GSLC) Gold Certification

Author: David Todd, DTodd@MastersProgram.SANS.edu
Advisor: Stephen Northcutt
Accepted: February 15, 2016

Abstract

It is the Chief Information Security Officer's (CISO) responsibility to identify the gaps between the most significant security threats and vulnerabilities, compared with the organization's current state. The CISO should develop an information security strategy that aligns with the strategic goals of the organization and sells the gap mitigation strategy to executive management and the board of directors. Before embarking on this new adventure, clearly articulate what success looks like to your organization. What is the result you are driving to accomplish? Then develop a strategy to get you there. Take a play directly from the Sales organization's playbook – Know yourself; know your customer; and know the benefits from your customer's perspective. Following this simple strategy will help the CISO close the deal of selling your Information Security Strategy.

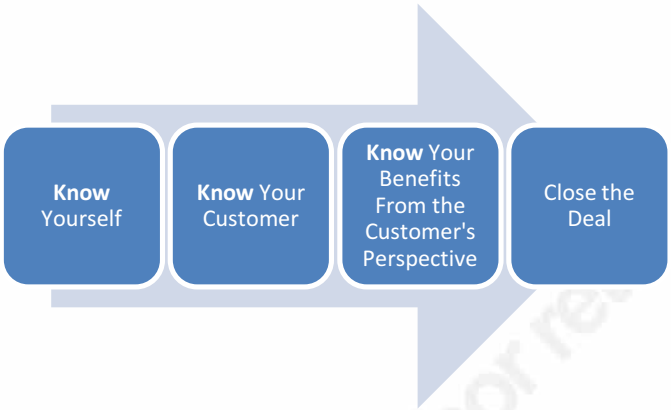
1. Introduction

During a recent budget review meeting, each department head was asked to present their annual budget projections and justify each initiative with a business case, supported by a sound return on investment analysis. The Information Security department was in the queue to present their budget recommendations immediately following the presentation by the Vice President of Sales. With visual aids, stories about recent client interactions, and even a few jokes, the VP of Sales explained how the initiatives he was presenting would help the company increase sales over the next twelve months, improve customer retention numbers, and increase engagement scores for his inside sales team. The net result would be a 20% increase in profits over the next three years. He went on to say that customers were demanding these new features, and if the organization didn't deliver, they would begin to lose customers to the competition. All of his projects were approved.

Next up, the Chief Information Security Officer (CISO) presented a new and improved Security Program intended to reduce the risk of an attack by a social engineering technique called "phishing." Attackers might exfiltrate customer or employee data from the organization to sell the information on the black market. Before the presentation even got into some of the exciting details about the phishing campaigns, new hire training videos, and lunch and learns being planned for the next year, the CEO asked, "So how again will this project increase profitable growth in our organization?" The focus of the company strategy was clear. The strategy was to get the company back on track to profitable growth by increasing revenues through more efficient processes, reduced expenses, and driving new business through exciting new features offered to customers. The CISO did the best he could to explain the benefits of the security program and how it would reduce risk to the organization, but with eyes glazed over, and people looking exhausted, the meeting eventually ended. The CISO returned to his office again this year without getting his key project approved.

Why didn't the Security program get approved, and why did the Sales department receive approval? Was it simply that the CISO's projects weren't as exciting? Take a

lesson from the Sales organization when delivering and gaining the support of your security strategy. Learn from what Sales did right in selling their initiatives to the executive team. The VP of Sales used a plan that had four distinct steps: Know yourself, know your customer, know your benefits from the customer's perspective, and finally close the deal.



The first step towards meeting the objective of selling your security strategy is to know yourself. "Find yourself. Be yourself. Sell yourself. Trying to do otherwise is a real waste of time. Embrace and celebrate all that you are. Be the best version of you and people will want to do business with you" (Eklund & Littlefield, 2015, p. 22). Knowing your personal strengths and weaknesses and how others perceive you is critical to knowing "how to begin the conversation" (Rackham, 1988, p. 12) on selling your security strategy. The VP of Sales knew his strengths and weaknesses. His relationship-building mindset, his ability to engage others in building a sound financial business case, and his public speaking talents allowed him to get his points across to the CEO and executive team in a precise, more understandable fashion.

Secondly, you need to know your customers, which will require "the creation of collaborative, trust-based relationships" (Ernst & Chrobot-Mason, 2011, p. 134) with your peers, senior executives, and the board of directors. In the book Boundary Spanning Leadership, the author goes on to say that in today's corporate environment, "you are required to do more than build trust with the individuals within your team. You also must build strong, trusting, and confidence-based relationships across the many groups and teams that constitute your organization" (Ernst & Chrobot-Mason, 2011, p. 135). CISOs have the responsibility to bridge the gap between technology and business acumen

and reach their executive teams and boards with the necessary cyber-security awareness to help organizations achieve their business objectives.

Lastly, the VP of Sales sold the benefits of his initiatives in terms understood by his customers, and not by trying to sell his logic of why the Sales actions made sense for the organization. In the book *How to Win Friends and Influence People*, Dale Carnegie cites Kenneth M. Goode from his 1929 book *How to Turn People Into Gold* where he says "that success in dealing with people depends on a sympathetic grasp of the other persons' viewpoint" (Carnegie, 1984, p. 161). Bottom line, the VP of Sales had a message that resonated with the CEO and others because the message, in this example his business case, had a direct relationship with the strategic direction and goals of the organization. The VP of Sales was able to close the deal.

2. Take a Lesson from Your Sales Organization

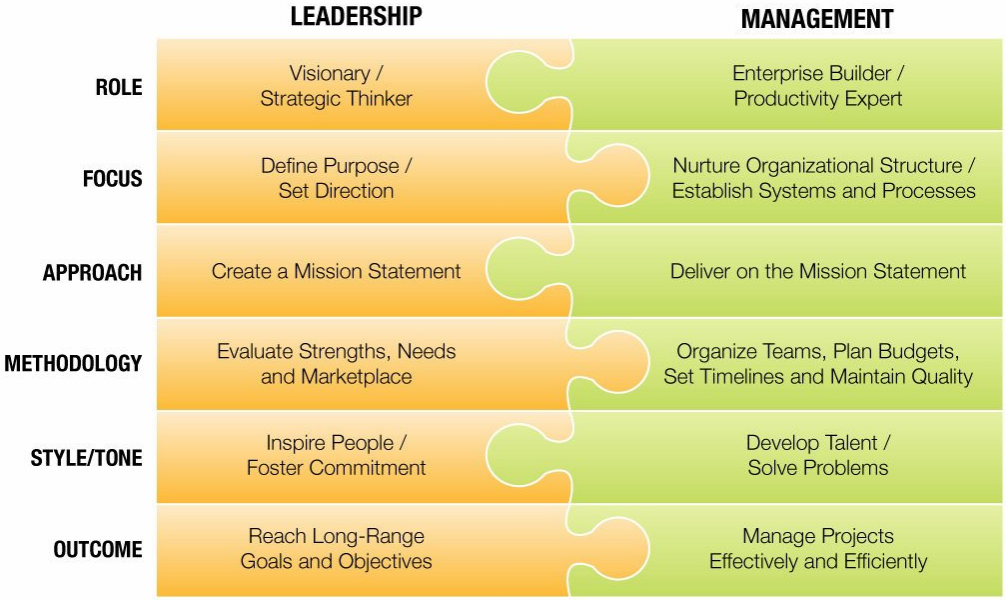
2.1. Know Yourself

"Most people don't move because they are de-motivated by their self doubts, which they turn into negative convictions" (Hopkins, pg. 77). The CISO can't walk into a budget meeting or the boardroom with self-doubts. Understand what your strengths and limitations are and do something about it. In The 7 Habits of Highly Effective People, Stephen Covey refers to this as "sharpening your saw" – or Habit #7. Covey says that "the single most powerful investment we can ever make in life – investment in ourselves, in the only instrument we have with which to deal with life and to contribute. We are the instruments of our own performance, and to be effective, we need to recognize the importance of taking time regularly to sharpen the saw…" (Covey, 1990, p. 289).

Let's be honest. You owe it to yourself, your team, your organization, your shareholders, and your customers. They are counting on you to deliver an environment where their data and investment is secure, and an environment where the business can thrive. Finding the balance between being secure and supporting organizational objectives is critical. It starts with you being you. Fredrik Eklund is one of the nation's most successful real estate brokers and star on the Million Dollar Listing New York TV show. He said that "Being unaware of your strengths and weaknesses, likes and dislikes,

abilities and inabilities is like trying to drive a car without gas. You can push the pedal, flash the lights, and spin the wheel all you want, but you're not going to get anywhere" (Eklund & Littlefield, 2015, p. 1). Is public speaking your Achilles heel, especially in front of executive management or the board? Maybe the anxiety is because you are trying to be someone else and not yourself. If so, you need to make executive management and the directors to "stop seeing you as an anxious, quivering wreck and instead start seeing you as the confident and charismatic person you are. Only then do they want to deal with you" (Eklund & Littlefield, 2015, p. 22). So do something about it. Join a local Toast Masters group or attend Dale Carnegie training and begin the journey of discovery to hone the skills necessary to deliver your important message with confidence.

In addition to being self-aware of your strengths and weaknesses related to your technical skills, business case analytical proficiencies, public speaking abilities and general self-confidence, it's important to understand what kind of executive you are. Are you an inspiring leader or a manager? There is a distinction between a leader and manager. Peter Drucker explains the difference this way: "Managers do things right, leaders do the right things" (Hesselbein & Cohen, 1999, p. 38). As outlined in the table below authored by leadership coach Chuck Gold, the functions of a leader and manager are interdependent. Both sides are needed for the organization to thrive (Gold, 2013).



David Todd, DTodd@MastersProgram.SANS.edu

If you are an aspiring leader, there's a period of exploration that goes well beyond book knowledge, classroom training, mentoring, and copying techniques or advice from others (Hesselbein & Cohen, 1999, p. 42). There's the need for self-awareness that drives one to be more than average, but great. Passion and drive are the foundations for leadership. So back to the original question, are you a manager or leader? "Don't confuse leadership with skills and systems or with tools and techniques. They are not what earn you the respect and commitment of your constituents. What earns you their respect in the end is whether you are you. And whether what you are embodies what they want to become" (Hesselbein & Cohen, 1999, p. 42).

Sharpen your skills wherever necessary and be committed to being that confident, inspiring leader. Don't copy someone else's style and behavior, but be yourself and make a connection with your customer. Know yourself.

2.2. Know Your Customers

One can usually find the corporate-wide objectives on the company intranet, company internet or public news feeds. Or maybe you are one of the fortunate CISOs that have a "seat at the table" and are a part of decision making to help set those organizational targets. Either way, to successfully align your information security strategy with organizational objectives, you must find out what your company's vision, mission, and goals are for the next year and beyond.

2.2.1. Build Relationship with Senior Executives

Request to meet with the CEO and the rest of the C-suite to understand their short-term and long-term priorities. Requesting this meeting within your first 90 days on the job as CISO is certainly the best approach. However, if you've missed that opportunity, it's never too late; the questions just have to be revised to make the process relevant to your particular situation. Senior level executives are usually open to demonstrate their support for information security by giving you some time. Don't focus on yourself, but focus on the executive's needs, and let them drive the conversation. One strategy is to ask each executive the same set of questions. Asking questions allow you the opportunity to evaluate their respective answers at the end of the process to identify

any trends. Take good notes. It's also important to understand that most executives feel uncomfortable talking about information security because it can be such a technical topic. Now is not the time to demonstrate to the executive your vast amount of security knowledge, but to understand their needs and concerns. Ask the same set of questions of the CEO and to each of his/her direct reports. Some suggested questions are:

1. What are the two or three biggest challenges the organization is facing? Why?
2. What's important to you and the board?
3. How are company goals and strategies established?
4. What are your expectations of the CISO?
5. If you were in the CISO role, what would you focus on first?

Now that you have a foundation of information from each of the C-suite executives, start looking for some common themes. "History tells us that at the heart of any effective organization, community, or society there are people and groups that come together to accomplish something larger or greater than what they could have accomplished alone" (Ernst & Chrobot-Mason, 2011, p. 127). What did you learn from your C-suite interviews about biggest challenges: declining sales, increased expenses, obsolete technologies, or possibly even cyber risk? Whatever it is, there is the opportunity to bridge commonality between the Information Security organization and your business partners.

2.2.2. Build Relationship with the Board of Directors

Build a relationship with your board. Do they understand and agree with where you are heading with the Information Security program? Boards have a fiduciary responsibility to understand and support management in their cybersecurity risk mitigation efforts. Many directors serve on multiple boards and, therefore, have the unique experience of knowing how various companies are managing their cyber risks. The National Association of Corporate Directors (NACD) is an organization that has as its mission the desire to develop exemplary board leadership. In their guidance to their members, the NACD highlighted five principles to help boards balance "cybersecurity with profitability" (Risk Oversight, 2015). If you understand these principles, you can

use this information to make an emotional connection with your board members. These principles are:

> **Principle 1**: Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
>
> **Principle 2**: Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
>
> **Principle 3**: Boards should have adequate access to cyber-security expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
>
> **Principle 4**: Directors should set the expectation that management will establish and enterprise-wide cyber-risk management framework with adequate staffing and budget.
>
> **Principle 5**: Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

(Risk Oversight, 2015)

If boards aren't talking about cyber-security, then they are already behind. Boards are getting bombarded with guidance from the NACD and financial publications such as the Wall Street Journal regarding their responsibility as directors to ensure cyber awareness. In a recent Wall Street Journal article it was stated that "Most CEOs and other executives have basic cyber awareness – they know that the failure to adequately protect critical assets could have a devastating effect on their business. But many of them are still limited in their knowledge of cybersecurity and do not know how different threats may affect their respective businesses." CISOs have the responsibility to bridge that gap between technology and business acumen and reach their executive teams and boards with the necessary cyber-security awareness to help organizations achieve their business objectives.

2.2.3. Information Security Steering Team

Build a strong cross-functional security steering committee comprised of senior level decision makers from across the company. Ensure adequate representation for each of the CEO's direct reports. The Security Steering Committee (the "Committee") is responsible for representing their respective business areas in overseeing the Enterprise Information Security strategy and manages to an acceptable level, the risks that may adversely affect the company's ability to achieve its objectives. The Committee should focus on competencies, capabilities, and effectiveness related to Information Security Strategy. Most often, the core of the security program is referred to as the C.I.A. triad – that is, ensuring the Confidentiality, Integrity, and Availability of your organization's information assets and resources.

- Confidentiality – protection of information from unauthorized persons or systems.
- Integrity – protection of information from unauthorized changes, whether intentional or accidental.
- Availability – accessibility of information assets and resources by authorized users whenever needed.

Particular attention is required to ensure alignment with the Information Technology organization. The NACD concluded that "cybersecurity as an enterprise-wide risk management issue, not just an IT issue"; however, a successful information security program relies on the cooperation and support of the Information Technology organization. In the development and enforcement of your security program, it is important to form a strong Information Security / IT partnership quickly. Information Security establishes and should be held accountable for the requirements, and IT is the enabler of those requirements. Let IT do what they do best – focusing on the technology necessary to meet the requirements driven by the Information Security organization. Partnership boundaries seem so black and white, but often where Information Security ends and IT ownership begins is a very gray area. That is why a strong partnership between the two groups is so important. Don't get caught in the turf battles often seen between these two groups.

3. Know the Benefits from the Customer's Perspective

3.1. Begin with the End in Mind

In Stephen R. Covey's book *The 7 Habits of Highly Effective People*, he explains Habit #2: "to begin with the end in mind means to start with a clear understanding of your destination. It means to know where you're going so that you better understand where you are now and so that the steps you take are always in the right direction" (Covey, 1990, p. 98). This section will help us understand a common flaw that most CISO's make when promoting their Information Security Strategy. Board members, senior executives, shareholders, and customers want results. We need to answer the question for ourselves and then articulate it to them: What does success look like when it comes to cybersecurity strategy?

The CISO needs to sell a clear and safe passage to those identified company targets in the terminology known and understood by the business. That's something most senior executives and board members can get excited about and support. They don't care nor have the time to understand the details of data encryption, multi-factor authentication methods, and intrusion detection systems. They want assurance that the CISO has a plan in place that removes those obstacles (aka "risks") that may block them from reaching their company goals.

As it relates to cybersecurity, success is probably the same for most organizations – mitigate the potential impact that a cyber breach has in achieving organizational objectives (COSO-guided Cybersecurity: Risk Assessment, January 27, 2016). However, how one reaches success is different for every organization. If the end is mitigating the potential impact, then we need to understand what controls, processes, and technologies are in place currently and evaluate their effectiveness in meeting the defined end goal. A comprehensive risk assessment can help one understand current state in contrast with end state expectations. Mary Galligan, Deloitte Advisory director at Deloitte & Touche LLP in Cyber Risk Services, suggest that "companies should consider directing investments at the risk assessment process itself" (COSO-guided Cybersecurity: Risk Assessment, January 27, 2016).

3.2. Sell the Benefits

One of the biggest mistakes made by most CISOs is that they try to sell the benefits from their technical perspective and not from the perspective of the customer. Customers, in this case your board and executive management team, don't typically talk nor understand "tech-speak". However, this is the language of the CISO. As exciting as it may seem to you to talk about the latest threats, tell horror stories about recent breaches, and show off the latest gadgets and tools to combat cybercrime, this information just does not resonate with the average executive or board member. Security initiatives can't get approval anymore based on FUD (fear, uncertainty and doubt). CISOs need "to come up with the same justifications as any other business unit, complete with the dreaded metrics, or hard financial facts" (Computerworld, July 24, 2003).

Don't try to sell intrusion detection systems, encryption methodologies, and multifactor authentication solutions to board members. These may all be good solutions that need to be updated or implemented within your organization, but it's not what executives want to hear. What you need to sell to your executives is an emotional connection to your plan for a clear and non-obstructive path to ensuring that the company meets its goals and targets. This may seem counter intuitive and just not logical. "Logic in sales is a gun without a trigger. You can twirl it all you care to but you can't fire it. Emotion is another gun in sales and this one has a trigger" (Hopkins, 1982, p. 46). CISOs should define a plan that has an emotional connection to achieving company targets. Executives get excited about increased sales, customer retention, reduced expenses or increased market share.

Let's review the security triad known as C.I.A. (Confidentiality, Integrity, and Availability) that was discussed earlier. Considering just one example, "availability", what is the value to the organization of one hour of processing up-time to your customer as it relates to sales generated? The dollar volume of sales or online quotes per a 24-hour period can be easily determined by working with the appropriate business areas. If the CISO wants to implement several solutions to combat denial-of-service attacks on the organization, then sell those initiatives in terms of reducing the risk of lost revenues due to downtime. Let's assume history at your organization shows that the company is losing

an average of 5-days per year due to continued denial-of-service attacks, costing the organization $1 million dollars per day in lost sales. The CISO is proposing a solution that will reduce the likelihood of a denial-of-service attack by 50%.

Be prepared to get into the technical details if asked, but the emphasis should be on selling a solution that will increase revenues by $2.5 million dollars per year (average of 5-days per year of down-time or $5 million total in lost revenues, reduced by 50% or $2.5 million). Assuming the proposed mitigation plan to reduce the impact of denial-of-service attacks is a $1 million one-time expense and $100,000 per year of on-going expense to maintain the solution, the Business Case can be easily calculated. In this example the first year benefit would be increased revenues of $1.5 million, with an on-going year over year benefit of $2.4 million per year of increased revenues. Using the potential for increased revenues approach allows you to sell the benefits from your executive's perspective, and not your own.

4. Conclusion

Take a lesson from your Sales organization when it comes to selling your Information Security strategy to executive management and the board of directors. Sales organizations have developed a model that not only works for selling your final product to your customers, but also on selling the benefits of their initiatives to executive management.

First, know yourself, which includes your strengths and weaknesses. Don't try to copy someone else, because the effort will come across superficial and tedious. CISOs must learn how to present their business case, so if public speaking is your weakness, then do something about it and improve those skills. Over time and by practicing, these skills can be learned and developed. Bottom line, be yourself and don't shy away from being unique.

Secondly, know your customer. For the CISO, your customers are your peers across the organization, other business units, executive management, shareholders, and most certainly the board of directors. Several approaches were discussed to develop

better relationships with the heads of each business unit, executive management, and with the board. Remembering what you learned about "knowing yourself" find an approach that best works for you and implement it within your organization. Some good approaches discussed included establishing an Information Security Steering team, implementing some regular cadence for a meeting with the CEO and his/her direct reports, and developing a strong working relationship with the directors on the board.

Lastly, we can learn from Covey's book The 7 Habits of Highly Effective People to "begin with the end in mind" (Covey, 1990, p. 98). CISOs can't keep trying to convince boards and senior leadership that we need more encryption, better firewalls, or intrusion detection systems. Most executives just don't speak that language. CISOs need to learn how to speak the language of the people with whom they are selling the Information Strategies. Sell them, again, not on the technologies, but on the benefits of the information security strategy. How will the implementation of the strategy help increase sales, or reduce expenses, or improve processes across the organization to help companies reach their targeted objectives? That's what needs to be sold to close the deal.

David Todd, DTodd@MastersProgram.SANS.edu

References

Carnegie, D. (1984). Pathways to Success: The Groundbreaking Best Sellers How to Win Friends & Influence People How to Stop Worrying & Start Living, Complete in One Volume. Hauppauge, NY: Dale Carnegie & Associates.

COSO-guided Cybersecurity: Risk Assessment - Deloitte Risk & Compliance - WSJ. (2016, January 27). Retrieved from http://deloitte.wsj.com/riskandcompliance/2016/01/27/coso-guided-cybersecurity-risk-assessment-2/

Covey, S. R. (1990). The Seven Habits of Highly Effective People: Restoring the Character Ethic. New York, NY: A Fireside Book.

Cybersecurity: What the Board of Directors Needs to Ask. (n.d.). Retrieved from http://www.theiia.org/bookstore/product/cyber-security-what-the-board-of-directors-needs-to-ask-download-pdf-1852.cfm

Eklund, F., & Littlefield, B. (2015). The Sell: The Secrets of Selling Anything to Anyone. New York, NY: Penguin Random House.

Ernst, C., & Chrobot-Mason, D. (2011). Boundary Spanning Leadership: Six Practices for Solving Problems, Driving Innovation, and Transforming Organizations. New York, NY: McGraw-Hill.

Gold, C. (2013, January 7). Leadership vs. Management | Champions for Growth. Retrieved February 1, 2016, from http://www.championsforgrowth.com/leadership-and-management-complimentary-partners-forever-connected/

Hayden, L. (2010). IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. New York, NY: McGraw-Hill.

Hesselbein, F., & Cohen, P. M. (1999). Leader to Leader: Enduring Insights on Leadership from the Drucker Foundation's Award-Winning Journal. San Francisco: Jossey-Bass.

Hopkins, T. (1982). How to Master the Art of Selling. New York, NY: Warner Books.

Rackham, N. (1988). SPIN Selling. New York, NY: McGraw-Hill.

Risk Oversight. (2015). A Guide to Risk and Its Governance in Financial Institutions Risk Management at the Top, 11-13. doi:10.1002/9781118497449.part1

David Todd, DTodd@MastersProgram.SANS.edu

Wilson, M. J. (2003, July 24). Calculating Security ROI is Tricky Business. Retrieved January 31, 2016, from http://www.computerworld.com/article/2572081/security0/calculating-security-roi-is-tricky-business.html

David Todd, DTodd@MastersProgram.SANS.edu