Information Systems Security, 16:257–263, 2007

ISSN: 1065-898X print/1934-869X online
DOI: 10.1080/10658980701746577

Taylor & Francis
Taylor & Francis Group

Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO Must Ask Each Other

Todd Fitzgerald
National Government Services,
Milwaukee, WI, USA

INTRODUCTION

The chief executive officer (CEO), chief information officer (CIO), and chief information security officer (CISO) walk into a bar. The CEO orders a light beer. The CIO normally orders his full-bodied stout beer but being politically savvy and noticing the CEO's order, also orders a light beer. The CEO's order has raised the curiosity of the CIO, and he just can't help but ask the CEO, "Why not have a real beer, one with all the flavor and the way beers are *supposed* to be made?" The CEO explains that there is just as much flavor for her needs, but with a much lower personal cost to the waistline. A few seconds later, the CISO comes in and orders a double shot of whisky and downs it in one gulp. The CEO turns to the CISO and says, "Did you have a bad day, is there something I should be concerned about?" The CISO replies, "No, I just saw that you ordered a light beer and figured we would be doing some belt-tightening, the business was losing money, you would cut my budget, and we are probably going out of business.

Was the CIO trying to be in touch with the needs of the CEO? Was the CISO overreacting? We have all heard many different versions of bar jokes; however, each reminds us there are simple lessons to be learned. Let's examine the roles of the CEO, CIO, and CISO further to understand their real roles within the organization necessary to move the business forward with respect to information security.

THE CEO, ULTIMATE DECISION MAKER

The CEO is faced with challenges and opportunities on a daily basis. The CEO may be oriented toward improving efficiency by reducing administrative costs as in the previous bar example, or may be confronted with challenges of merging with another organization, increasing revenues by a certain percentage, improving market share, or introducing new innovative products for the company. A CEO's role is to create an inspiring vision and mission for the organization and to ensure that the actions of the culture match this vision. Consider the difference in culture between a processor

Address correspondence to
Todd Fitzgerald, CISSP, CISA, CISM,
Medicare Systems Security Officer,
National Government Services,
(Subsidiary of WellPoint, Inc.),
6775 W. Washington Street,
Milwaukee, WI 53214
E-mail:
Todd_fitzgerald@yahoo.com or
Todd.fitzgerald@wellpoint.com

of health-care claims, and that of a company such as Apple, which produces the popular iPod. The former may be very focused on providing excellent customer service at the lowest possible administrative cost, while the latter may be focused on creating an environment where creativity and innovation can flourish. This does not mean that the health insurer does not care about innovation or that the iPod manufacturer does not care about costs, but rather that the emphasis in priorities and the subsequent decision-making is likely to be consistent with the most important values.

The CEO is the big-picture person. So what should be their role with respect to security? Equal support. Equal support means that the CEO should be expected to 1) support the security department's initiatives as they relate to the mission of the business, 2) ensure responsible funding is provided for ongoing security operations, and 3) hold the components of the business accountable or achieving their objectives in a secure manner. In other words, the responsibility of the CEO to security is no different that their responsibility to any other part of the business or any other executive. Consider that you are the CEO in charge of manufacturing an automobile. While you may be responsible for meeting quarterly sales and production goals at a tactical level, the key role is to ensure that, over time, the company continues to produce automobiles demanded by consumers over the long term at a reasonable profit to attract investors and create sustainable shareholder value. While a great design could take many years and multiple focus groups, and could be built with the highest quality imaginable by spending more in production and time, the reality is that the car may never make it to market in time or may cost too much if these parameters are ignored.

Since the CEO is dealing with financial, operational, and business risk decisions on a continuous basis, he or she needs to have enough information to make a fact-based decision that will not expose the organization to regulatory compliance issues, risk to the business reputation, or decrease the efficiency and effectiveness of the organization's capability to produce. When launching a new product or service, if there is not a clear understanding of the security risks, the organization could end up closing its doors due to the lack of controls.

Many CEOs today are aware of the security risks which have created financial and public relations nightmares related to the loss of information. Astute CEOs take the time to understand this risk and ensure that appropriate responsibility is designated for reducing the risk. The stories of data loss that have been in the news are endless—Card Systems is out of business after 40 million customers were potentially exposed, TJX stores incurred a large financial impact after 45 million customers had their credit card accounts exposed, Bank of America had 1.3 million people exposed due to a missing backup tape, Eli Lilly disclosed confidential information in an email to approximately 700 people on Prozac, which ended up costing millions in fines and oversight by the Federal Trade Commission for 20 years. The key takeaway from these stories is not so much in the exposures themselves but rather that these are events which have setup the "potential" for real loses by the consumers. A much smaller fraction of actual personal damages really occurs. The message for the CEO is that once the breach happens, the possibility of a loss by a customer sets off a chain reaction of events which involve costly public relations, incident response, increased audits, implementation of additional processes, people and technology, offering free credit monitoring, and so forth. This does not include the intangible costs that much management and technical staff attention is focused away from the core business issues to respond to the security event. Money is also diverted from projects, or projects are delayed to enable the mitigation of the incident.

Funds are a finite resource within any organization. The CEO must weigh the costs of a breach and the costs of other initiatives, and decide the appropriate amount to be spent on information security. Typically, after an incident, the checkbook seems to be open. When nothing is going wrong, the question may become, do we have too much staff? Could we do this for less? This makes providing the appropriate amount of information by the CISO to influence the CEO a challenging task. Security is a typically viewed as a cost to the business. There is nothing sexy about a security project, as in and of itself it does not produce increased revenues or reduce costs for the organization. Revenues produced are a result of the products and services that are created, and administrative costs are a result of the assets,

1. How will this security investment reduce my business reputation risk? How will this keep our name off TV, newspaper headlines, and blogs on the Internet?
2. How will this level of funding ensure that our organization maintains an adequate control environment, which ensures that I am performing the documented activities on a consistent basis?
3. Will our security controls meet the regulatory compliance requirements we are exposed to (GLBA, SOX, HIPAA, FISMA, PCI Standard, etc)?
4. What level of funding are our competitors doing?
5. How will this investment support a key product or service that supports our corporate vision?
6. Will these investments have an impact on the reduction of ongoing audit issues?
7. Is there support from the other executives for this investment?
8. Can this investment be performed at a lower cost by an external consultant or outsourcing the process?
9. Does this investment require a multi-year commitment?
10. Are there short-term paybacks which can be realized through a phased project implementation?
11. What other resources within the organization are required?
12. Where is this type of security investment on the adoption curve? In other words, are we an early adopter (higher risk, such as an Identity Management effort), or is this a more mature practice (lower risk, such as implementing anti-virus/IDS technologies)?
13. Do we have the skills within our organization to adequately execute this investment or is additional expertise needed to lower the risk?

FIGURE 1 **Questions the CEO Should Ask the CISO**

people, or processes eliminated or reduced. Security investments are a choice for the CEO, not an absolute. Just as other departments may implement technology or create efficient manual processes, there are trade-offs. The CEO should be asking questions of the CISO when security investments are being solicited, as shown in Figure 1.

The CISO needs to be able to provide the CEO with the answer to the most important question, "why." Even after an incident occurs at a competitor company within the same industry, the "why" is still not necessarily a given. The CEO should challenge the current control infrastructure, soliciting input from the CISO, the CIO, and the business executives to ascertain whether or not the event could happen within their organization. It may be that the current level of security investment is still appropriate and additional funding is not needed. It may be that the security area is not spending money in the highest risk areas and funds need to be re-allocated.

The CEO is interested in the security light beer. What is the minimum amount of funding that is necessary to provide the needed taste, without having to take away from the other goals of the organization (through allocation of fewer resources to other areas, in turn reducing their ability to meet their goals of maintaining a healthy waistline for the organization).

THE CIO, WHERE TECHNOLOGY MEETS THE BUSINESS

The role of the CIO has evolved over the past 15-20 years to the point where in medium and large organizations the existence of the role is expected. In some respects, the evolution of the CISO is following a similar path of 1) an understanding that the role is needed, followed by 2) role ambiguity, 3) maturation of the role to be the intersection between the business and the technology vs. being the most knowledgeable technology person in the organization, and eventually 4) obtaining an executive presence on par with the business executives and being "invited to the table" so to speak. Much of this evolution in today's world can be attributed to the significant role that technology plays in business effectiveness and efficiency.

While the earlier staffing of the CIO came predominantly from the information technology ranks, and more specifically, from those individuals responsible for running the data center or in charge of development of the mission-critical applications for the business. These areas were chosen for their knowledge of how technology supported the business (applications) or how to run the IT business (data center operations). In today's environment, the CIO is just as likely to be chosen from the business side of the house, as they bring with them the knowledge of "what" needs to be accomplished through information technology. In the end, the "how" is figured out by the middle and first line management and their technical staffs.

Some organizations still run with an IT focus at the CIO level vs. a business focus. In either case, CIO is usually under pressure to 1) deliver the projects on time and within budget to the business, and 2) to ensure availability. Most IT projects involve a high degree of variability and interdependencies

and rarely meet time and budget estimates. To manage the variability, project goals must be developed to constrain the deliverables. The security implications are that in order to meet the deadlines, security investments must be pragmatic and be introduced at the appropriate time during the project lifecycle. For example, if the security department first reviews the implementation of access controls during the testing phase, the project team will not be excited about having to go back and rewrite code to meet the "new security requirements." As an alternative, if security is represented on the project team during the initial analysis and design phases, the project can proceed without these roadblocks. The CIO needs to ensure that a system development life cycle is followed and the appropriate parties and deliverables are identified to avoid this situation. Attention to security should be on a risk adjusted basis, with the higher priority projects receiving increased, formalized attention, while the smaller efforts could be accomplished by the development team through the use of internal peer reviews of the security requirements.

Since availability is critical to the organization, the CIO must ensure through a Business Impact Analysis (BIA) that critical applications are identified, along with their Recovery Time Objectives (RTO) to ensure that there is minimal impact to the business in case there is an outage or disaster. This will involve working with the business to determine their priorities. The CIO must also ensure that servers are configured according to documented baselines, applications are coded using secure coding techniques, access to the networks by third parties are controlled, and both internal and external audit issues are followed up promptly by IT management. Each of these items not only supports the confidentiality and integrity security requirements but also reduces the risk of unexpected unavailability. It is a given these days that proper investments must be made in firewalls, anti-virus software, spam filtering, and spyware. Many of the security vulnerabilities identified through penetration testing or vulnerability assessments are typically the result of failure to analyze what settings were appropriate or failure to consistently adhere to a defined process, not that more technology was necessary. Purchasing an elaborate aggregation tool for logs is of little value if the most important events have not been identified or no one is reviewing the logs on a consistent basis.

1. What is the minimum necessary effort required to produce code that is secure?
2. What do we need to do to avoid audit issues in the application development process without adding significant expense or delays to our projects?
3. Do you see your role as an after-the-fact reviewer of security controls or engaged in the implementation of the controls?
4. What technologies are available to reduce the labor intensive process of keeping up with the latest patches, system vulnerabilities, configuration management and compliance monitoring?
5. Can you provide information on the "real risks" that are present in our specific industry and the appropriate implementation alternatives that companies use to mitigate these risks?
6. How can we ensure that we have reduced our exposure to an acceptable risk?
7. What tangible benefit will we receive from the security investments that will enable the business?
8. Which internal/external audit issues will these investments eliminate?
9. What other information technology resources are required, in addition to ssstems Security staff, to implement the security solution presented? What support is required from the business?
10. How do the security requirements integrate with the systems development life cycle? Are we performing these tasks already?
11. Do we have the necessary experience in-house to implement these solutions? Should we consider outsourcing some of the functions?
12. What are the critical success factors for achieving success in our security efforts? How much security is "enough"?
13. How can you help reduce the time I spend on compliance-related efforts in gathering documentation and audit samples?

FIGURE 2 **Questions the CIO Should Ask the CISO**

The informed CIO understands the impact of not performing all of these tasks and the impact it can have in causing unexpected downtime.

Just as the CEO must be aware of the external environment, the CIO must be able to solicit accurate information from the CISO to obtain knowledge as to the risk of doing nothing and what issues the competitors are facing. Some of these questions that the CIO may want to ask the CISO are shown in Figure 2.

When the Veteran's Administration lost a laptop containing personal information on 26 million individuals, and subsequently required that all of their laptops be encrypted, many organizations took notice. While security programs should not be run by the "incident of the week," due to the widespread

media coverage, such major incidents put the CIO in the position of having to answer the question "could this happen to us?" Savvy CIO's will not want to accept the risk of this type of situation and will require his IT management and Systems Security develop a proposal with several different cost alternatives that would mitigate the problem.

The CIO may find himself from time to time serving in the role of arbitrator between the IT management and systems security for security issues. IT projects are driven by deadlines to produce the required functionality. As a result, shortcuts may be taken in the testing, change control, documentation, peer review, or training processes in preference to spending more time and resources in the code development process. Shortcuts in these areas can lead to segregation of duties issues, lack of appropriate documentation, and lack of evidence that the correct processes were being followed. For example, live production data may have been used in the testing environment, potentially disclosing more information than needed-to-be-known by the developers. Additionally, change control procedures may not have been followed by the server engineers, thus increasing the possibility that the baselines are not matching the intended configuration. This also increases the risk that external auditors will not have the documented evidence necessary for their review.

CIO's have a responsibility for sustaining the information technology investment on behalf of the business, and to ensure that the information is being made only available to those who are authorized in a secure manner. It is a continuous balancing act of allocating the appropriate resources to systems security, while ensuring that ample resources are available to operate the infrastructure and create new functionality through innovative business applications for the business.

The CISO, Protecting the Business

Unlike the bar scene that was painted previously, the CISO must have a sense of what the real risks are to the business and not feel that every event has the ability to cripple the business. True, budgets do get cut, performing more with less money that was provided the prior year is often times expected in business, and security is no exception. It is only logical, as increasing numbers of security investments are made, that a point is reached where the cost of maintaining a service should be less than the cost to build the service. Imagine building a complex interstate highway interchange with supporting bridges over a period of several years. The costs are typically very large for engineering, moving the soil, removing the old infrastructure, moving the new beams in place, constructing the bridge and managing traffic flow during the process. To support the bridge in an ongoing manner, periodic road surfacing, bridge inspections, and repainting of the lines are necessary; however, this amount is much smaller than the original investment to construct the bridge. Security works the same way, and CISOs must be able to separate 1) new investments that provide increased functionally and 2) support for the ongoing security operation. After the initial "we better fix our security program and do something" dies down, the CIO and CEO will be expecting that costs are managed efficiently and either more work is being performed at a level cost, or the costs are reduced. Implications for the new CISO are that this lifecycle of spending should not be unexpected. Since security departments are typically considered overhead, a cost center, or a non-revenue producing department, pressures to cut any unnecessary costs will be continuous. As the old adage is applied here, that a "good day" for the CISO is when nothing happens, it is a challenge to be rewarded with increased investments for "nothing happening" when other departments are investing to make things happen.

The CISO has the opportunity to talk about the technical controls in place in the organization with technical detail to the CIO and CEO or he has the opportunity to communicate how his or her department's activities contribute to enabling the delivery of the latest new company product. The savvy CISO provides information related to the later or shows how they are reducing ongoing costs, reducing the wait time necessary for business user access to systems, or reducing the lost productivity which happens as a result of a virus. The CEO may be interested in how the government regulatory compliance requirements are being satisfied or how the audit issues are being reduced year to year. The CIO may have the same desires for information, as well

as how well the security area is working with the other IT management areas.

Security has become a broad discipline with the CISO responsible for facilitating the implementation and ongoing compliance with the multiple domains of the common body of knowledge, such as risk management, operations security, physical security, business continuity, laws and ethics, network security, and so forth. The person performing the role of the CISO may or may not have that title and may be named Security Director, Security Manager, or Information Security Officer. The exact title is not as important as the appointed responsibility for protecting the organizational assets. Obviously, detailed expertise for these domains resides in many different individuals. The CISO is expected to have broad security knowledge and why each of these areas are important to the business. The ability to work up and down the organization, translating technical jargon into a language appropriate for the CEO, CIO, business executives, middle management, end users, and external parties is an essential skill. Leadership involves the influencing, written and oral communication skills, and building relationships with business partners for the bigger picture (of supporting the vision and mission of the business). Just as the CEO and CIO have questions for the CISO, the CISO must be able to ascertain what is going on in the business to adequately support the mission. Some answers the CISO may want to obtain from the CEO and CIO are shown in Figure 3. The CISO should have a sense of the answers for some of these questions before approaching the CIO and/or CISO , so that an effective conversation can ensue. However, the questions should still be asked, as the CISO may have some blind spots or filters which my cause invalid assumptions. After all, they are key stakeholders of the security services and the best way to find out what the customer wants is to "ask them."

In effect, the CISO is the cheerleader for risk management, utilizing the "tools of security." They are expected to keep abreast of the current security approaches within the industry and recommend the appropriate measures for their particular organization which match the organization's appetite for risk and ability to commit the resources. CISOs should always recommend multiple cost/risk alternatives, because in the end, it is the business executives and the CEO who must ultimately decide how much risk to take. The role of the CISO is to inform, not decide, albeit influence the decision when it appears that the organization is taking on an excessive risk posture which it may not clearly understand.

1. What are the top three business priorities within the next 12-18 months?
2. If we could develop and implement solutions for two security issues tomorrow, what would they be? In other words, what are your biggest pain points?
3. What would be the best way to engage you to ensure that you get what you expect out of the information security program?
4. What level and frequency of reporting would you like to see? What metrics would be the most meaningful to you? (Note: The CISO should present examples of the types of metrics that may be meaningful as a starting point.)
5. What is the period of time that you expect medium and high-risk issues identified by the internal/external auditors to be resolved by the organization?
6. How involved in the development of the information security policies would you and your management like to be? Engaged in the development? Formal approval? Informed? Additionally, what resources are you willing to commit and at what organizational level?
7. What have you read in the news that you wouldn't want associated with our company?
8. Would you characterize our organization as an early adopter, innovator or follower utilizing mature technologies?
9. Would you characterize our organization as a risk-taker or risk-averse?
10. What are your expectations for how information security can support the organizational goals within the next 12 months? 18-24 months? Beyond three years?
11. What products or services would you like to be able to provide right now, but are apprehensive due to the perceived security exposures?
12. If we were to have a significant incident happen to us, what are your expectations of my area? Other business areas? Where does the responsibility lie?
13. How else can I help you?

FIGURE 3 **What the CISO Needs to Learn from the CEO/CIO**

FINAL THOUGHTS

In a sense, the CEO, CIO, and CISO are each running a business with a vision, mission, and a set of operating principles, policies, and procedures for effective and efficient operation. There is conflict when the norms of the three individuals and their supporting organizations are not aligned with each other. Information technology and security provide

support to the business and only exist because of that relationship. The business vision and mission must drive the projects, the risk profile, and the investments required. Each individual is responsible for different facets of information security, from establishing and maintaining an organizational culture which supports the activities, the implementation of secure technology projects, to the ensuring that ongoing security operations are appropriately managed. While the CEO and CIO roles are more clearly defined due to the maturity of the job description, the CISO continues to evolve. One thing for sure is that if the organization's culture leans toward efficiency and orders a light beer, the CISO would be better off not assuming the sky is falling and work in partnership with the CIO to develop cost effective security strategies. And maybe once in awhile that security project with a little stout in the funding might even come along!

BIOGRAPHY

Todd Fitzgerald, CISSP, CISA, CISM serves as a Medicare Systems Security Officer for National Government Services, Milwaukee, WI which is a subsidiary of WellPoint, Inc, the nation's largest Health Insurer. Todd is an Associate Editor of the ISC2 Journal, a frequent international, national and local speaker, as well as an author of information security management issues. Todd is the recipient of several information security awards, including as a 2005 Midwest Information Security Executive of The Year Finalist. Todd is also co-author of the book, CISO Leadership: Essential Principles For Success (Auerbach, 2008).