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

The chief executive officer (CEO)
Chief information officer (CIO)
Chief information security officer (CISO)

The CEO, Ultimate decision maker

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.

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.

The CEO should be asking questions of the CISO when security investments are being solicited, as shown above:

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?

The CIO, Where technology meets the business

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.

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.

Questions the CIO Should Ask the CISO

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?

The CISO, Protecting the Business

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 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.

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.

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 systems, or reducing the lost productivity which happens as a result of a virus.

What the CISO Needs to Learn from the CEO/CIO

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?