Hey, Boss – How are YOU protecting our Information and Networks?

Affecting Positive Cyber Leadership

By Andrew Vonada

Regardless of the size of the organization, business leaders carefully craft their leadership styles and shape the messages they communicate to those in their charge. Countless hours are consumed with both the science and art of business management. Performance based mathematical measures are developed and analyzed in detail; images of CEO's, sleeves rolled up, in animated conversation with employees are regularly woven into internal and external marketing materials. Further, conducting regular, face to face, and open conversations with employees is a widely accepted practice, if not the norm for senior managers today.

However, during one of those conversations, how well prepared are senior leaders to answer the question: "What are you doing to protect my personal information and the company's proprietary data?" The ability to answer that question is essential to any business leader's credibility and is a barometer of their success in the information age – regardless of the audience.

All businesses have stakeholders that include employees, Boards of Directors, partners, customers and investors. Therefore, all senior leaders, particularly those at the top of the organization, are expected to articulate the financial status and functional posture of their respective businesses to their business' stakeholders. These messages must include both current detail and future plans, and more relevant to this article, they must be expressed in the first person.

It is unlikely any successful senior leader would survive their first Board of Directors presentation if they lacked firsthand knowledge of the financial and operational state of the company. In today's environment, that's not the full story. It is fair to say that leaders (not just senior executives) must have continual awareness of the security and status of their networks and data. Network and data security are no longer just supporting administrative functions; they constitute key strengths and vulnerabilities. Since a leader is held accountable for everything that happens and fails to happen, it is no longer acceptable to merely allow the individual charged with *IT* responsibilities to be the sole source of knowledge or accountability. Firms can endure market fluctuations – they cannot easily endure a major breach or compromise of their systems and data.

That said, a business leader does not have to be deeply educated or experienced in the unique language and processes affecting these essential business functions. Those skills are very specialized and the cyber environment is incredibly dynamic. Nevertheless, leaders must be able to address this vital business function. They must define their individual role and guidance, as well as what the organization is doing as a whole. Establishing that capability requires several steps on the part of business leaders and the management must be a top-

down driven function. The urgency and visibility is further amplified if network support services are contracted to an outside vendor.

Network and data security has rapidly become a vital function of any business. Leaders must be informed and proactive. Therefore, below are recommended steps to reinforce their position and help mitigate the effects of a negative event.

Establish a direct rapport with your information security lead. Regardless of the size of your organization, it should be clear who has this vital charge. Further, there should be no doubt about the importance you place on cyber security, and exactly what you expect from them. This can include any direct reporting or communications deemed necessary to satisfy your comfort that the right things are being done. Additionally, you can leverage greater company-wide emphasis by the perceptions that accompany the increased attention.

Know enough to ask and answer questions. You don't have to know how to write code or be able to cite the properties of the most recent version of network protection tools, but you do need to know enough to appreciate the practical implications of cyber security related measures. This will further enable you to answer employee questions (particularly from those familiar with the subject matter) and provide credible responses.

Know what level of protection you really need. You need to provide information security protections commensurate with the risk and magnitude of the potential harm to your collective network. Those risks can result from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of your organization, and on information systems used or operated by your organization or by a contractor.

Publish and actively execute an Information Security Program. Ensure through your personal directive that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of your organization. Further, security controls must be integrated with strategic and operational planning and reflect your organization's strategic requirements. Further, senior managers must have the necessary authority to execute the Program to secure their respective operations and assets – don't plan or execute your Information Security Program in a vacuum.

Lead by example. If cyber security is important to you, then don't send a representative to key meetings or delegate critical decision-making authority to a subordinate. Strictly adhere to the policies and standards that bear your name; set an individual standard for rigor that meets your expectations for the team.

Publicly elevate your attention to data and network security policies, reporting, and accountability. When you make information security a priority, it reinforces the efforts of your designated information security lead. More specifically, require your information security lead, in conjunction with other senior managers, to provide regular reports addressing the

effectiveness of the Information Security Program, including the progress of remedial actions. Further, ensure training is conducted to support compliance with information security policies and standard, and that YOU are a visible participant.

Regularly audit your network safeguards and policies, and ensure the results, along with any corrective actions are delivered directly to you. While you trust and value your accounting staff, you still insist on regular audit practices to ensure the validity of their activities. The same should be true with the critical cyber infrastructure your organization relies on for not only the integrity of your data, but also the continuity of your operations.

Weave network and data security into your messages to <u>all</u> stakeholders. Take advantage of any opportunity to bolster confidence and invigorate vigilance. This is another vehicle to stress the level of importance you place in the integrity of your business in an increasingly scrutinized cyber environment. It has to be readily apparent to every stakeholder that you take this subject seriously and it has your attention.

Develop a credible and sufficiently detailed *Information Security Elevator Speech*. This does not need to be a doctoral dissertation. Instead, craft a two or three sentence message that accurately reflects the state of your network and what active measures you are taking to remain secure. This also serves as another vehicle to demonstrate that cyber security is important to you and why.

The risks for subordinating or ignoring network and data security are significant, and regret is a terrible thing. If your enterprise realizes a compromise, you should strive to eliminate the soul searching associated with the post-event scrutiny of your cyber security posture and policies. Instead, apply a message of confidence that you have been proactive, and that through personal example, you can demonstrate to your stakeholders your diligence and rigor. In turn, this will allow you to concentrate on mitigation and not suffer the burden of developing a philosophy and program after the fact.

In the end, senior leaders must visibly and continually emphasize that cyber security is an essential business function, and back that message up with credible policies, actions and accountability.

Mr. Vonada is the President and CEO of JB Management, Inc. (JBM). Headquartered in Alexandria, Virginia, JBM has more than 25 years experience providing collaborative and innovative support to clients worldwide. To learn more about JBM, visit: www.goJBM.com