



A View from **the Board**

The board of director's agenda has changed radically in the past two years thanks to Sarbanes-Oxley and a host of other privacy and security regulations. Board meetings that used to focus on forward-looking strategy now concentrate on regulatory-related operational details. The shift has been uncomfortable

for most board members, particularly as concern for their own personal liability has mounted.

Today, board members have skin in the game. So much so that *Harvard Business Review* ran a case study in 2003 in which several experts advised readers not to join public boards. Their conclusion: It's just not worth the risk.

But seasoned infosec leaders recognize the seismic shift and have altered their approach to the board accordingly. They recognize that they are speaking to a nervous, impatient audience. Use of FUD—fear, uncertainty and doubt—may help garner short-term support for security projects, but it will likely undermine their program's long-term viability, the presenter's credibility and, perhaps most damaging, the board members' willingness to remain on the board.

"Many technical managers rely too heavily on the FUD factor to sell the urgency of information security," says Michael Brown, assistant vice president/information security officer for the Federal Reserve Bank of Chicago. "After the Y2K fiasco, senior leaders are not much buying into fears associated with what most perceive as 'IT issues.' SOX compliance has given many security executives a new bat for swinging."

Although SOX and other privacy and security regulations may seem like champions for information security, it is critical that infosec leaders understand how these new requirements look from the board's perspective.

"I think people are more cautious about becoming board members," says George Dalton, founder and CEO of Novo1, a direct-response marketing company. Dalton, who sits on several public boards, served as the CEO and chairman of Fiserv, a publicly traded information management services provider to the financial and health benefits industries, for more than 20 years.

"I think a number of board members are becoming disenchanted because of the portion of time security-related topics occupy during the meetings," Dalton says.

Board meetings take two to three hours longer than they

did a couple of years ago, he observes, with most of that time spent poring over audit-report details.

"Nobody likes that," Dalton adds. "We need to listen to the findings. But the findings, although important, are not strategic. If you look at your average board members, they are not normally tactical people. They are action-oriented decision makers."

Perhaps the most confounding aspect of the new board meetings is that these highly experienced board members want to con-

Leveraging the board's expertise starts by sharing with its members your two-to-three-year information security road map.

tribute. They are eager to share their experiences and help the companies they serve. Yet in the current model, there is nothing they can do about the audit findings other than make recommendations for personnel changes. Their job is to sit and listen.

When reporting to the board, ground yourself in this simple realization. If you are only presenting historical data points, or worse yet FUD, board members aren't likely to actively engage. They'll do their duty to listen. But this fails to leverage the board as the asset it is. It also contributes to their mounting discontent.

Leveraging the board's expertise starts by sharing with its members your two- or three-year information security road map. By explaining how your organization's recent actions and immediate plans fit within a broader, longer-term context, you will gain credibility and engage your audience. Ultimately, this will make the experience mutually rewarding, because you will have provided the board members an opportunity to do what they do best—provide hard-earned insight and sound strategic counsel.

E. Kelly Hansen is CEO of Neohapsis, an information security consultancy and enterprise IT product-testing lab. Write to her at khansen@neohapsis.com.