Managing Expectations in a Changing World

Problem identified and communicated, plan created, funds provided, problem resolved. This is the lifecycle senior business leaders often expect – and prefer – organizational challenges to have. It's the way decisions are made and issues addressed for many functions of the business.

By Marleah Blades

Unfortunately, this leads senior management to expect a similar lifecycle of security-related challenges: 1) Security apprises management of threats and vulnerabilities. 2) Management allocates funds to address them. 3) Problem solved.

However, it's rare that you can honestly say "problem solved" in security. Every little shift of the business, every new program or policy in a single department, every new piece of hardware and software installed, every external change to the market, global politics, even the weather – every one of these has the potential to introduce new threats and vulnerabilities into the organization's risk environment, sending the security leader back to the C-suite to say, "It's changed. We need more."

At the same time, management's baseline awareness of many security-related issues is high, due in part to a 24-hour media machine and an increased focus on risk brought on by the economic recession and other factors. "Management understanding is creating a new era in leadership expectation," said Bob Hayes, Managing Director of the Security Executive Council.

Engaged management knows about many of the threats to business and expects security leaders to efficiently and cost-effectively manage the risks they face, and that's a good thing. However, security leaders must take special care in this environment to communicate the inherent limitations of their craft. If they don't, those high expectations could turn into unrealistic mandates.

John McClurg, VP and CSO at Dell, spoke briefly about this challenge during the Next Generation Security Leader final session. McClurg has led successful security and risk functions at Honeywell International and Lucent Technologies, and he is a co-chair of the Overseas Advisory Council. Lately, he has found himself appreciating a new the impossibility of 100-percent protection.

"In recent years I've been humbled by the new vision and understanding I have of the incredible prowess and discipline of the adversaries," he said. "Notwithstanding our best efforts and our communication with leadership as to the nature of threats and vulnerabilities, it's not a question of 'if' but 'when' we're compromised.

"This is exacting of us more attention to the way we message what we need and what that expenditure can be used to produce in the near term. It also requires a clear, honest declaration of the prowess and ingenuity of the adversaries," McClurg continued.

It's an interesting challenge to strike a balance in communication that inspires confidence in security's ability while clearly laying out the limitations of that ability; that avoids using fear to influence support while ever reminding management not to get too comfortable about their security.

According to McClurg, "Whatever mechanisms you use to brief management on the threats you see emerging – bolster those conduits. So it may be that you increase the frequency of briefings because of the speed at which the change is occurring. What may have been adequate as an annual brief may now require quarterly or semi-annual updates. Even the tone of the message may need to be adjusted. The common phrase you hear is that we should under-promise and over-deliver. But we even need to be careful of what we think 'under-promise' means."

In communication and in action, security must focus not only on mitigating risk, he continues, but "on how resiliently we've positioned ourselves to move and adjust, and how well we have thought through the way we architect our structures and enclaved our most critical assets, to decrease the likelihood that the inevitable compromise will result in unacceptable loss."

"A conservative position one might adopt," says McClurg, "is to try to focus on the actuality while poised agilely to respond to the theoretical possibilities for which you haven't expended funds. In that environment particularly you may have to request funds more frequently, but hopefully if you explain that strategy, [management] will understand that you're trying to control spend in an environment in which you could easily spend endlessly." SECURITY

About the Author:

Marleah Blades is senior editor for the Security Executive Council, a leading problem-solving research and services organization focused on helping businesses effectively manage and mitigate risk. Find out more by e-mail contact@secleader.com or visit https://www.securityexecutivecouncil.com/sm. You can also follow the Council on Facebook and Twitter.