SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Converging Risk Assessments

Marleah Blades

Originally Published in Security Today

August 2008

Converging Risk Assessments

Just as every business is unique, so too are corporate approaches to physical and logical security convergence. However, as companies develop their convergence models, they should thoroughly consider all business functions or processes that may benefit from it, says John McClurg, vice president of global security for Honeywell.

McClurg, a member of the Security Executive Council, has seen a variety of models as he's researched convergence practices in large organizations, and he's noted that corporations frequently overlook one function that could benefit from convergence: risk assessment.

"Classically, your IT risk assessors will go to part of a business, show up one week and then come back and issue a product," McClurg says. "A couple of weeks later your physical team will come, take more of your time, do an assessment and issue a product. It's left to the [assessed department] to correlate the total risk posture."

At Honeywell, McClurg has pulled those two activities together, cross-training risk assessors and sending out teams able to perform a single comprehensive risk analysis comprising both IT and physical security. He's seen a number of benefits from this innovative approach.

A Clearer Risk Picture

"The converged assessment is more likely to present in a coherent manner the interdependencies between physical and cyber vulnerability," McClurg says.

"A good example is the phreakers (telecom hackers) I used to work against when I was in the FBI," he said. "They would exploit a 30-year-old rusty lock with an old-fashioned pick set -- a physical world vulnerability. Once that's exploited, the phreaker goes into the central office of a phone company and quickly gathers up manuals, passwords and other equipment that he can take back to his base of operations, and there advance a far more sophisticated cyber attack than he would ever have been able to do but for the physical world deficiency."

When IT and physical risk assessments are done separately, the assessed business unit has to put the two assessments side by side and analyze them carefully to discover interdependent vulnerabilities -- but this doesn't happen often. A converged assessment draws the lines of interdependency for the business unit, leaving less to the imagination and allowing it to move directly to the mitigation phase.

Better Audit Performance

Because the converged audit provides a clearer risk picture, it helps each business unit prepare more thoroughly for the corporate audit, anticipating which issues might be cited and dealing with them in advance. When one team is responsible for risk assessments, it is also easier to coordinate them with the corporate audit schedule in mind.

"We know where [the audit is] going to go a year in advance," McClurg explains. "And we try to get our assessments pre-positioned six months in advance of the audit so any remediation that needs to be done can be fixed before they come. You see a more robust audit rating and less going to audit committee."

A single converged risk assessment causes less interruption, improving unit productivity. McClurg says Honeywell also has experienced significant cost savings from using converged risk assessment teams.

"With a team that is cross-trained, you can do more with the same individuals," he says.

Significance Of Influence

To begin converging risk assessments in the corporation, you must have a relationship and influence with the heads of other business units and in the executive suite.

"I sit on [Honeywell's] IT Council with the CIO and its Technology Leadership Council with all the CTOs, and I advance those duties as a peer, which conceptually pulls or expands the way you traditionally think of the CSO," McClurg says."It's a positioning that acknowledges that in this day

and age security is not an afterthought but an inextricable, indispensable way of advancing the business, whether it's the technology or the IT or the resiliency piece of the business.

The inextricable nature in which security weaves itself into the company justifies the placement of this critical role."

Because of his role in the organization, McClurg has found strong support for converging risk assessments: "I end up not having to do nearly as much pushing as I'd otherwise have to do, because as you educate your peers, they start to recognize the need for certain initiatives, so they're pulling with you instead of being pushed."

About the Author

Marleah Blades is senior editor for the Security Executive Council, a problem-solving research and services organization that involves a wide range of risk management decision makers. Its community includes forward-thinking practitioners, agencies, universities, NGOs, innovative solution providers, media companies and industry groups.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com