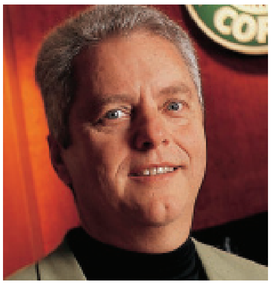
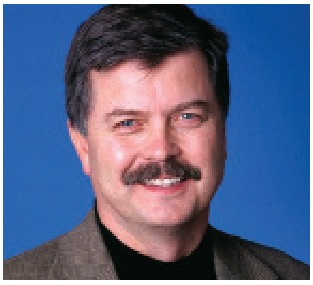


Francis D'Addario, *Security Executive Council Faculty, Former CSO, Starbucks*



Philip C. Aronson, *President and CEO of Aronson Security Group*

Ray Bernard, *Security Executive Council Expert Faculty and President, Ray Bernard Consulting Services*

Bud Broomhead, *CEO, Intransa*

How can I make a strong case for a security project that is innovative and forward-looking rather than reactive to a specific event?

Our analytical capability for measuring both risk mitigation and value contribution is essential for making the persuasive business case. Typically, we leverage past success for forward-looking opportunity.

When my security department led cross-functional teams against the workplace violence risk in the 1980s and 1990s, we were able to demonstrate injury, cash loss and turnover reductions with an estimated 250-percent return on investment at Southland, Jerrico, Hardees and Starbucks. Those results were, in turn, leveraged for improved hiring diligence, fraud detection and network exception reporting. Each demonstrated incremental loss avoidance and return.

Evolving compliance or mitigation requirements are subsidized when we make leadership clients aware of measured investment performance using a relevant cross-functional stakeholder approach. Risk mitigation enables the business plan. Brand reputation benefits from improved safety, loss avoidance and cost improvement. Our relative success begets proactive security re-investment.

One of the brutal facts that we in the security industry must acknowledge is that Security is stuck in a narrow definition of value around risk and impending risk.

Thus, it is difficult to make a compelling business case for any innovative idea.

The way to make a strong business case around a proactive project is to avoid this pitfall. Don't focus on just risk mitigation — focus on how this project will increase business value.

Define your project in terms of how it will align to your organization's mission, vision, values and goals.

Expand the range and scope of your idea to benefit the entire organization rather than providing "security for security's sake."

We at ASG insist on looking at a project holistically to make sure that we can offer an innovative approach to security that makes sense from a business prospective.

The job of security is to reduce security risks to acceptable levels at an acceptable cost, in a manner harmonious with the business. This is the concept that most of today's security practitioners have regarding the security function.

It is also true that the general role of any business function or unit is to enable or execute the mission of the business. That gives the security practitioner a secondary purpose, and with today's networked technologies, there are non-security benefits that security technology can bring to the business.

These are the areas in which a security practitioner has a mandate to be proactive: reducing risks (which includes increasing security effectiveness), reducing costs and adding value to the business. A strong business case for any proposed security initiative will be based on one or more of those, and will educate management if they are not already aware of the needs or benefits involved.

When you are planning a proactive project, or preparing to take preventive measures, it is important to anticipate coming conditions — upcoming events, and the state of the social and economic environment — and to then project how those conditions will impact security for the company and employees.

From that, you can deduct what measures can help you avoid those potential problems.

But how do you justify those measures to management?

Try to get your project on the revenue side rather than the cost side.

A lot of risk management is about cost avoidance and cost cutting, which is hard to measure in verifiable amounts.

Getting your project cast in the light of how it will enhance the brand, improve the customer or employee experience, or enhance the company's product offerings will give your business case a positive impact rather than negative one.

Next Month's Question: From a risk management perspective, how is security in cloud computing different from security in outsourced services?

For more information about the Security Executive Council, please visit www.securityexecutivecouncil.com/?sourceCode=std.