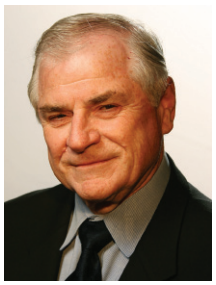
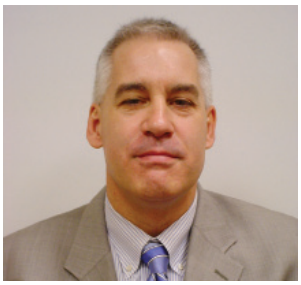


Richard Lefler, *former CSO, American Express, Dean of Faculty, Security Executive Council*

Bob Hayes, *Managing Director, Security Executive Council*



Michael Philips, *Director of Corporate Security, Bose Corporation*

Denise Reubens, *Sr. Director Global Security, Microsoft Corporation*

How do you define the cost of security?

The traditional measurement of security costs includes operating costs, capital investments that measure what a company spends to protect its employees, brand reputation and often, customer relationships.

Businesspeople are trained to analyze the return that a given investment will yield, and often, if that investment does not meet the company "hurdle rate," the investment is not made.

Measuring security returns is difficult for businesspeople because security programs prevent problems and financial losses (often measured as variable costs). So how do we measure the absence of a problem as a worthy return on investment?

One idea that seems to be resonating is to do risk assessment relative to the security exposures the company faces in achieving its business goals. Then design mitigation programs to offset specific risks that cannot be managed with other risk management solutions like, for example, insurance.

In effect, this shifts the focus to managing the risk exposure, instead of managing the cost.

During any persuasive executive presentation on security programming or initiatives, you can count on being asked how your idea or proposal compares to others in the industry and how the cost compares to your peers'. For decades, this has been problematic because of a total lack of common industry benchmarks and information sharing. There is no area in which this lack of shared definition is more evident than in determining the cost of security.

To complicate matters even further, there has never been more intense interest on management's part in understanding and comparing these costs. This is due in part to the significant increases in total security budgets (often due to consolidating functions/services into security) in many companies over the last 10 years.

There is now an opportunity to participate an initiative underway to define and establish benchmarks for the "Total Cost of Security." It will be the first to account for costs associated with individual programs/services by facility, location, country, business unit, differing cost centers and other organizational variances. To receive the results of this groundbreaking research, you must participate.

How to define the cost of security will differ for each company, depending on factors such as the company culture and executive management's perception of how increased or decreased security will mitigate risk.

The greater the risk exposure in any given area, generally the more funds will be allocated to mitigate those risks, or the more security will cost financially. However, company executives may choose to accept certain risks and not to allocate funds to mitigate them.

Periodic risk assessments must be undertaken and the results presented to executives in order to keep them current about the risks to their business.

As security professionals, our greatest goal is to reduce security risks at our companies at a cost that is acceptable to our executives.

In order to accomplish this goal, we must educate our executives about the company's level of security risk so that they can make the appropriate decisions.

The cost of security is a direct correlation to the ability to successfully identify, analyze and mitigate potential risks to your company. The business should prioritize risks by impact and likelihood and the opportunities to reduce, control and/or monitor these risks.

Robust planning with ongoing risk assessment, gap analysis, intelligence, exercising, tabletop training and program enhancements will increase your capabilities and effectiveness to respond, stabilize and recover during and after the time of an incident. In turn, this will reduce your overall response cost.

By documenting these actions, you can help make the business case justification for budget funding and resource requests. Then you can confidently present your funding requests knowing that senior leadership has the ability to rationally support your request and has the understanding to accept a specific risk or threshold of risk to the company.

Next Month's Question: How would you respond to a Web-based incident causing significant brand damage?

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