

<http://www.cioupdate.com/budgets/article.php/3590516>

You Get What You Pay For

By [Liz Roop](#)

March 9, 2006: CIO Update

For cost-effective security you have to consider more than just hardware and software

In a perfect world, cost would never factor into decisions regarding security. But no budget is unlimited, and today's CIOs must approach security with the same "more-for-less" attitude they do any other technology purchase.

With security, however, a decision based purely on dollars could wind up costing a company far more than bargain-shopping CIOs saved on the purchase—not to mention the future costs if a security solution can't grow with an organization's needs.

"Cost-effectiveness is a function of both what you spend and what you get," said Andrew Krcik, vice president of Marketing for encryption vendor PGP Corp. "Not spending enough to hit the minimum threshold buys you nothing. If you haven't put enough security in place to create a minimum level of quality and pervasiveness, why did you spend any money at all?"

To put the price of inadequate security into perspective, PGP commissioned a study by The Ponemon Institute to determine the actual cost of a data breach. The survey examined the costs incurred by 14 companies in 11 industry sectors with breaches affecting between 1,500 to 900,000 consumer records—a total of 1.4 million compromised records.

In general, the largest breaches occurred in financial services, data integration and retail sectors, while the smallest breaches were in higher education and healthcare.

What they found was:

- Total costs to recover from a breach averaged \$14 million per company or \$140 per lost customer record.
- Direct costs for incremental, out of pocket, unbudgeted spending averaged \$5 million per company or \$50 per lost customer.
- Indirect costs for lost productivity averaged \$1.5 million per company or \$15 per customer record.
- Opportunity costs averaged \$7.5 million per company or \$75 per lost customer record.

Those findings are a good illustration of why, when it comes to security, a solution must be far more than just affordable.

"It's all about minimizing loss and minimizing risk and exposure to risk," said Eric Ahlm, director of emerging technologies for Vigilar, a information security consultancy.

Evaluating Risks vs. Needs

There are five key considerations when it comes to evaluating the potential cost of a breach, according to Jim Reno, vice president of engineering for Arcot Systems, a digital signature and identity solutions vendor. These include direct and replacement costs for physical assets (including cash), as well as statutory costs such as fines.

Another consideration is the impact a breach will have on the business, including human resources and communications, lost trade secrets, sales leads, etc. Finally, consider the costs of the hit to a company's reputation.

"This is particularly relevant in businesses such as financial services which are highly competitive in the consumer space, and where switching costs for the consumer between institutions is relatively low, said Reno.

"Also important to note is the 'trust-factor' associated with the financial institution. Once this trust is damaged for a particular bank or brokerage in the eyes of the consumer, the relationship is difficult, if not impossible, to repair."

The potential costs of a breach need to be weighed against actual needs, which Reno said should include the following:

- Ease of use: If it is too difficult to use, people will try to develop workarounds.
- Education: Do people understand why there is a need for security and how the new solution will benefit them/the organization?
- Ease of integration: How does the security solution fit into the overall IT and business architecture, and how long and what will it cost to deploy? Can it be implemented in a timely and cost-effective manner with current personnel resources and equipment?
- Compatibility with business needs: Does the solution help meet the organization's current and future compliance needs? What applications beyond security alone can this solution enable to assist in the business processes of the company?

Knowing an organization's risk profile is also critical to the evaluation process, adds Ahlm.

"You need to really understand what's at risk and what the cost is in terms of tangibles and intangibles," he said. "But you've also got to be able to communicate that to the people who care. There's no generic answer for everyone. It's an approach, a framework."

The Process at Work

When the Georgia Technology Authority (GTA) worked through the security evaluation process recently as part of a wireless network deployment at the Georgia State Capitol Building, it had the benefit of hindsight on its side.

In 2003, the state's General Assembly deployed a wireless network that was almost immediately hacked. The resultant wide-spread publicity forced the WLAN to be shut down.

"It wasn't a network that we set up, but we took that as a lesson learned," said Al Yelverton, GTA's director of command center and network administration.

Thus, when Gov. Sonny Purdue charged the GTA with deploying a WLAN in 2005, the group knew security had to be tight, but it also had to be reliable, affordable and able to work through some very unique structural challenges. The building's three-foot-thick brick walls required a higher concentration of wireless access points to ensure reliability, which also made the system more vulnerable.

"Because we're the government, cost is always uppermost in our minds," said Yelverton. "But we didn't settle for the cheapest technology, we looked for a cost-effective solution."

Ultimately, they selected AirDefense Enterprise. That system met not only their security and monitoring requirements, but also provided a high level of scalability that would enable the GTA to expand wireless capabilities to other buildings.

As an enterprise-class solution, AirDefense is highly scalable, which is very appealing to CIOs in need of cost-effective solutions.

"Scalability, simplicity and inexpensive deployment," said Krcik of enterprise-level solutions such as PGP Universal, are what's needed as well as a platform capable of provisioning multiple encryption applications in a combination of gateway and end-point locations that provides a "deploy once, enable over time" approach.

Arcot offers a software-based system called ArcotID. From a technological standpoint, it acts as a smartcard, but instead of a piece of hardware, a small software file is loaded from a remote server onto the user's device or USB fob. A PIN is utilized in conjunction with the file for authentication.

"The software-based smartcard looks to an application exactly like a [traditional] smartcard, but from a user perspective, it's easier to use because they don't have to carry around an extra piece of hardware, said R. "Doc" Vaidhyanathan, Arcot's vice president of product marketing and corporate development.

At the end of the day, the actual cost of the solution is secondary to the needs of the business and the end user, said Krcik. A truly cost-effective security solution will not only carry a reasonable price tag, but will also limit the disruptions to day-to-day business activities.

"Ultimately, the cost of the software is a big consideration, but the disruption it causes to existing networks and infrastructures is (bigger), as is the impact it has on the user base if you have to train users; that's almost a non-starter these days. And then there are the operational costs," he said. "Those are the three major things an IT organization looks at; the cost of the software itself is often secondary."