You May Be Fighting the Wrong Security Battles

How IT executives can determine the right amount to spend—and where to spend it

BY LAWRENCE A. GORDON AND MARTIN P. LOEB

A recent wave of information-security breaches at high-profile companies has many executives on heightened alert. They're trying to figure out everything they can do to prevent breaches, limit the damage if one occurs, and be prepared to rebound quickly from whatever harm is done.

As they consider their options, two questions loom large: How much should they spend to protect their companies' information? And how can they get the most for their money?

Our research suggests they should spend substantially less than the expected loss from a breach, and perhaps spend it differently than many might think.

THE ONE-THIRD MARK

We developed a model to help executives determine the optimal level of investment to protect a given set of information—whether it's customers' personal information, company financial data, strategic-planning documents or something else. The model weighs the potential loss from a security breach, the probability that a loss will occur, and the effectiveness of additional investments in security.

One key finding from the model: The amount a firm should spend to protect information is generally no more than one-third or so of the projected loss from a breach. Above that level, in most cases, each dollar spent will reduce the anticipated loss by less than a dollar.

A second key finding: It doesn’t always pay to spend the biggest share of the security budget to protect the information that is most vulnerable to attack, as many companies do. For some highly vulnerable information, reducing the likelihood of breaches by even a modest amount is just too costly. In that case, companies may well get more bang for their buck by focusing their spending on protection for information that is less vulnerable.

WORKING IT OUT

The following four-step approach has proved useful in helping executives sort all this out:

Step 1. Estimate the potential loss from a security breach for each of the company's various sets of information. For starters, it's useful to simply categorize information sets as having either Low Value, Medium Value or High Value.

Step 2. For each set of information, estimate the likelihood that it will be stolen, by examining the probability of an attempt to steal the information and the vulnerability of the information to attack. Again, broad categories are useful: Designate each set of information as either Low Threat/Vulnerability, Medium Threat/Vulnerability or High Threat/Vulnerability.

To combine the two factors, assign each a numerical rating—say, on a scale from 1 to 10—and multiply the two numbers by each other.

Using that scale, you might consider any combined ranking below 30 to be Low Threat/Vulnerability, and any ranking above 70 to be High Threat/Vulnerability; different people will draw those lines in different places.

A key point: Information that is highly vulnerable to attack but unlikely to interest a hacker (think of a banged-up old subcompact parked with the keys in the ignition, in a high-crime neighborhood), or that is very attractive to a thief but is very well protected (a brand-new luxury car on the White House grounds), would fall into the Low Threat/Vulnerability category.

Step 3. Create a grid with all the possible combinations of the first two steps, from Low Value, Low Threat/Vulnerability up to High Value, High Threat/Vulnerability. Then plot each set of information on the grid. This gives a clear view of where the greatest potential losses lie—not just in terms of the cost of a breach, but also in terms of its likelihood.

Step 4. Focus spending where it can reap the largest net benefits—where a given amount of money will produce the biggest reduction in potential loss.

Security investments should continue to be made as long as the incremental benefits are greater than the incremental costs—which usually stops being the case where the costs are roughly one-third of the total expected loss from a security breach.

Security breaches can have a substantial negative effect on corporations. However, contrary to conventional wisdom, the overwhelming majority of security breaches have little economic impact on corporations—all the more reason to use this kind of cost-benefit analysis to allocate finite information-security resources.

However, this approach is best thought of as a framework, not a panacea, for making sound information-security investments. It is not a magical formula that can be used to churn out exact answers. Rather, it should be used as a complement to, and not as a substitute for, sound business judgment.

Dr. Gordon and Dr. Loeb are professors at the University of Maryland's Robert H. Smith School of Business and the authors of "Managing Cybersecurity Resources: A Cost-Benefit Analysis." They can be reached at reports@wsj.com.