ITSC

Understanding Information Security Economics 101

Forrester Information Security Report

Prioritizing Information Security requires CISOs to understand what their company's assets are worth, and how much they're willing to spend protecting them.

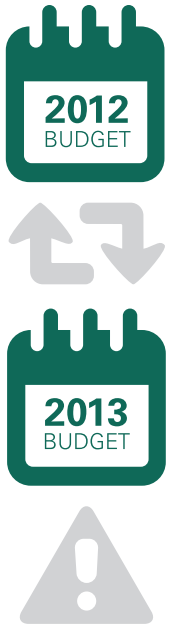
Key Points of Interest

- Know which assets are worth the most in revenue
- Know the costs of protecting these assets
- Security costs / revenue = information security value

CISO's are evaluated not only on technical performance, but also on how they manage information security as a business – prioritizing expenditures and making difficult financial decisions. These days, CISOs need a simple formula that they can use to estimate the financial value that information security delivers, and that will provide them a useful tool in demonstrating the return on proper information security investments.

The Forrester report, **"Determine Information Security Economics 101"** allows CISOs to put a monetary value to their information assets, map their spending on security and understand the actual security value of the company's information and IT assets.

ITSC, Information Technology Security Council
1268 Prospect Street, La Jolla, CA 92037 | tel 866.611.4652 | info@itsecuritycouncil.com



Put a Dollar Amount on the Information

The problem with determining where to spend an information security budget is that CISOs don't align security objectives with corporate, strategic or functional objectives. Many CISOs are unable to name their company's strategic objectives and most of them use few quantitative measures to support the budgeting process. Cybercriminals Monetize information; so should CISOs. The best place to start is to discover which information assets make the most money for the company. When assets are prioritized, security resources can be spent accordingly, using them where they're needed and not wasting them where they aren't.

One of the biggest mistakes that CISOs make is to use last year's budget to determine this year's. The problem is that using this approach doesn't show real budget needs. Instead of basing the current budget off of last year's guesstimates, quantifying company assets will give a real, concrete jumping off point for IT security expenditures. CISO's need to not only learn what their assets are worth but what the company is willing to protect them. Very few CISOs have accurate and comprehensive information on the type and location of the critical data that resides in their company's infrastructure, let alone how much protection that data needs.

Quantify Fixed Costs & Predict Variable Costs

Once the CISO has put a number on the company's information assets they need to estimate the costs of a breach. To fully understand the financial impact on an organization, CISOs should understand all the various costs involved in protecting their information assets. This includes the fixed costs as well as variable costs, especially those related to breaches. These costs include direct and variable costs (breach identification, forensic analysis, and remediation), variable legal and regulatory costs (payment of fines, penalties, and mandatory audits), variable operational costs (consulting, communications, outside legal counsel, new security processes, and new investments in technology) and variable reputational costs (what is the company's reputation worth, and how much of that will be left after a breach?)

Quantifying reputational costs may be difficult but it's important to understand the price of a company's reputation to know what will be lost when it's tarnished.

Insiders or Outsiders

Once the CISO understands the security costs and the value of their information assets, all that's left is to take that information and plug it into the following formula:

Security Costs / Revenue = Information Security Value

This will give an idea of the company's information security value, helping the CISO create a game-plan and allocate resources. In this formula, Security costs are the costs required to safeguard revenue-producing information assets and information with compliance and risk implications, and Revenue is the income produced by those assets.

Knowing security value allows senior executives to make better security decisions. They can easily understand that a product or solution is worth a certain amount to the company in future revenue and the percentage of that revenue they're willing to spend to protect it. In time, CISOs can learn to manage this ratio down, demonstrating a more focused and efficient use of resources.

The Take Away

The best security strategies require prioritization of company assets, only possible once the numbers have been run. There is enormous pressure on CISOs to create IT security strategies that run more efficiently and effectively than ever before. Discovering your information security value is a vital step in understanding how much to invest to protect your company's valuable information assets.

SOURCE - Determine The Business Value Of An Effective Security Program, Ed Ferrara. Forrester, October 2, 2012 www.forrester.com/Determine+The+Business+Value+Of+An+Effective+Security+Program+Information+Security+Economics+101/fulltext/-/E-RES82082?objectid=RES8208