The Return on Investment (ROI) of Pre-written Information Security Policies

In this paper we provide a simplified Return on Investment (ROI) calculation and justification for purchasing quality pre-written information security policies such as those found within *Information Security Policies Made Easy* (ISPME), by Charles Cresson Wood, CISSP. In this simple worksheet we will compare the total cost of policy development using ISPME to the cost of developing policies internally or using outsourced development.

Estimating the Costs of Policy Creation

There are many factors that go into the cost of developing and maintaining policies. (See our related whitepaper "*The Total Cost of Policy Development*") For example, Chapter 1 of ISPME lists the following critical steps in the policy development process, *before* you begin to write policies:

Table 1: Steps in the Policy Development Process [1]

Key Step
Establish the team
Gathering Key Reference Material
Preparing a topic coverage matrix
Make critical system design decisions
Structuring review, approval and enforcement processes
Plan for policy enforcement
Plan for rollout and education process

For the purposes of this discussion, we will limit our scope and only consider the cost of *writing* the information security policies. To make a cost estimate, we must make educated guesses at three factors: (1) The amount of policy material that needs to be developed, (2) the time required to develop and write the policies, and (3) the cost of development resources. Then we can make an estimate based on this formula:

Total Development Cost ($) = Document Length (pages) x
Time (hours/page) x
Cost ($/per hour)

Of course, this is a drastic simplification of the entire process and the related organizational costs, but it will serve to make a basic estimate.

Estimating Document Length

Of course, the number and length of policy documents will vary widely from organization to organization, depending on the size and scope of its business operations. To take a rough estimate for the total policy length (in pages) for a typical organization who wishes to follow a leading practices approach to security, we will consider only the sample policy documents that come with ISMPE. ISPME version 10 contains 15 completely pre-written policy documents, totaling roughly 100 pages of text.

Total Page Estimate: 100 pages

You can make your own estimate by taking the number of documents that must be created by an average policy length of 2-5 pages. As another benchmark, the ISO 17799:2005 information security standard [2] has 123 defined control areas. Even at one page per topic, total document length would be over 100 pages.

Estimating Total Development Time

Once again, the amount of time required to write one page of normal text depends on the skill and experience level of the individual. However, according to data from the STC (Society for Technical Communication), a typical amount of time required to develop one standard page of technical documentation is roughly 1 hour. Based on estimates from experienced policy developers, this number is more likely 2 to 5 hours per page. Although information security policies typically require a much higher level of editing and review, we will keep this conservative number to make our estimate.

Using our estimated document length from above, this brings the total time requirement to 100 pages at 1 hour/page, or 100 hours.

Total Time: 100 pages x 1 hour/page = 100 hours

Estimating the Cost of Development Resources

The cost of development resources once again depends on many factors. In the most conservative case, if we assume that a technical writer could perform this task, a good approximation would be roughly $50/hour. If this was a full-time employee, benefits loading would raise this to roughly $60/hour. However, even a well training technical writer will not have the IT and security skills required to create and maintain these documents. A more accurate number for a highly-skilled information security or IT professional would be $100-$150/hour. It is not uncommon for the real rates to be in the

range of $200-$400/hour. For the purposes of our discussion, we will assume the lower number of $100/hour.

Total Cost: 100 hours x $100/hour = $10,000.00

For any organization that has used an outside consulting agency to develop information security policies, this cost estimate is typical for about 10 pages of text, rather than 60. This mostly reflects the reality that there is much more preparation and review work to be done before actually writing information security policies. In most cases, however, management is unaware of these hidden costs and drastically underestimates the total cost to the organization. It is common for policy engagements with large consulting companies to run from $50,000 - $100,000.00

Comparison Cost Table

Method	In-house development	ISPME
Development Time	100 hours	0
Resources Required	1 person	0
Total Cost	**$10,000.00**	**$795.00**

If we plug more reasonable estimates for development time (3 hours per page) and resource cost ($150 per hour) we get the following:

Method	In-house development	ISPME
Development Time	300 hours	0
Resources Required	1 person	0
Total Cost	**$45,000.00**	**$795.00**

Further Cost Savings

In addition to the simple "brute-force" cost savings during the policy creation phase, purchasing a leading set of pre-written material such as ISPME has many other short and long term cost savings.   For example:

1. The policies found within ISPME have been used and proven effective by thousands of organizations around the world. It would take much iteration by a highly-skilled information security professional to create policies with this scope and level of quality.
2. The pre-written policies within ISPME provide a very fast time-to-value, allowing organizations to establish policies much more quickly and freeing up valuable internal resources.
3. Higher quality material from a reliable source will reduce the review and approval time of policy documents, getting policies in place more quickly and reducing the risk of control areas that may have been overlooked.
4. Policies need to be updated and maintained. ISPME is now in version 10 and provides regular updates as new technologies and risks are introduced.
5. ISPME policies are mapped to leading frameworks such as COBIT and ISO 17799, saving time during compliance efforts.

6. ISPME contains valuable advice on the entire policy development process that will save your organization many hours of experimentation and reduce the risk of failed policies that never get used by the organization.

Summary

In even the most conservative estimates, ISPME will save organizations thousands of dollars over the lifecycle of policy development. For an organization that has an average benefits-weighted employee cost of $100/hour, **ISPME will pay back this initial price investment in one business day**. Not only will information security policies based on ISPME be written and adopted much more quickly, they are based on leading practices that have proven effective over many years and for thousands of organizations.

References

[1] *Information Security Policies Made Easy*, by Charles Cresson Wood, CISSP, CISA, CISM. Published by Information Shield, Inc. 2002-2005. [http://www.informationshield.com]

[2] *ISO/IEC 17799:2005 – Code of practice for information security management* - ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission). Available at ANSI [http://www.ansi.org/]

About Information Shield - Information Shield is a global provider of security policy solutions that enable organizations to effectively comply with international regulations. Information Shield products are used by over 7000 customers in 59 countries worldwide. Find out more at our Regulatory Resource Center at www.informationshield.com or contact the author at dave@informationshield.com