Solution Brief

The Total Cost of Information Security Policy Management

InformationShield

About Information Shield

Information Shield is a global provider of security policy, data privacy and security awareness solutions that enable organizations to effectively comply with international security and privacy regulations. Information Shield products are used by over 9000 customers in 60 countries worldwide.

Information Shield, Inc.
2660 Bering Dr.
Houston, TX 77057
www.informationshield.com
sales@informationshield.com
P: 888.641.0505
F: 866.304.6704

Contents

1. Introduction
2. Total Cost of Policy Management
3. Initial Policy Development Costs
4. Ongoing Policy Maintenance Costs
5. Total Cost Savings
6. References

Information Shield Solution Brief

The Total Cost of Information Security Policy Management

By David J Lineman
Information Shield

Summary

This paper is designed to help organizations build a business case for the purchase of the PolicyShield Security Policy Subscription Service ™. To perform the business analysis, we develop a cost model for estimating the Total Cost of Policy Management (TCPM).

In this paper we compare the total cost of policy development using PolicyShield to the cost of developing and maintaining policies internally or using outsourced development. As the analysis shows, PolicyShield can save as much as $20,000.00/year in policy update and maintenance costs.

1. Introduction: The ROI of PolicyShield

This paper is designed to help organizations build a business case for the purchase of the PolicyShield Security Policy Subscription Service ™. To perform the business analysis, we develop a cost model for estimating the Total Cost of Policy Management (TCPM).

PolicyShield is the only service available that provides actionable, pre-written policies updated on a quarterly basis. In this paper we compare the total cost of policy development using PolicyShield to the cost of developing and maintaining policies internally or using outsourced development. **As the analysis shows, PolicyShield can save as much as $20,000.00/year in policy update and maintenance costs.**

Organizations that are just beginning to develop policies will obviously benefit from the wealth of pre-written security policies found in PolicyShield. However, even organizations with mature information security programs can benefit from the ongoing analysis and policy development resources of PolicyShield.

2. Estimating the Total Cost of Policy Management

To simplify cost our analysis, we can break overall policy management into two distinct phases: Initial policy development and ongoing maintenance.

In the development phase we focus on the resources and effort required to develop an initial set of written security policies that would be typical for an organization. In the maintenance phase we focus on the resources and activities required to keep the organization compliant with data protection laws.

3. Estimating Initial Policy Development Costs

There are many factors that go into the cost of developing and maintaining written information security policies. (See our related whitepaper "The Total Cost of Policy Development") For example, Chapter 1 of Information Security Policies Made Easy by Charles Cresson Wood 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. The amount of additional organization effort required to review, approve, and publish policies will depend greatly on the size and scope in the enterprise. 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 simplification of the entire process and the related organizational costs, but it will serve to make a basic estimate of initial development costs.

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 that wishes to follow a leading practices approach to security, we will consider only the sample policy documents that come with PolicyShield. PolicyShield contains 20 completely pre-written policy documents, totaling roughly 150 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

Development Comparison Cost Table

Method	***In-house development***	***PolicyShield***
Development Time	100 hours	0
Resources Required	1 person	0
Total Cost	**$10,000.00**	**$1600.00**

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***	***PolicyShield***
Development Time	300 hours	0
Resources Required	1 person	0
Total Cost	**$45,000.00**	**$1600.00**

This cost is more in-line with a typical engagement with a third-party consulting firm. In these cases, policies are often written from “scratch” after a lengthy interview process.

4. Security Policy Updates and Maintenance Costs

Initial policy development is only part of the cost. Security policy development is not a "one-time" process. In order to reduce risk of data breaches keep the organization compliant with data protection laws, written policies need to be periodically updated. (See our whitepaper, "The Need for Updated Security Policies" [3] for a review of the business case for updated policies.) In Table 2 we outline some of the basic steps involved in a policy review and update process.

Table 2: Steps in the Policy Review and Update Process [3]

Key Step
Re-Establish the team
Review New Organizational Risks
Review Regulatory Changes
Review Key Incidents
Policy gap analysis
Write new policies
Review and Approve Policies
Publish and Educate Users on new policies

PolicyShield can help organizations identify new risks that are likely to impact written information security and data privacy policies. Each quarter, the PolicyShield Subscription is updated with new pre-written information security policies designed to address new risks to the organization. These risks include:

1. **Compliance Risks** – Change in regulatory frameworks that may impact required policy controls.
2. **Technology Risks** – Introduction of new technologies (such as wireless devices or mobile phones) that present new risks to sensitive information.
3. **Environment Risks** – New threats evolve as criminals become more sophisticated and exploit new technology. PolicyShield includes written policies in response to real-world security incidents.

PolicyShield can significantly help the organization in several key steps of the policy maintenance process outlined in Table 2. The following table shows an estimate of the development time for each phase of the policy review and update process for a typical organization.

Maintenance Cost Comparison Table

Activity	***Effort Per Quarter***	***Cost***	***PolicyShield***
Review Regulatory Changes	8 hours	$ 800.00	
Review New Technologies	8 hours	$ 800.00	
Review Major Incidents	4 hours	$ 400.00	
Write New Policies	12 hours	$1200.00	
Map to Frameworks	4 hours	$ 400.00	
Total Cost	**40 hours**	**$ 4,000.00**	**$400.00**

Using an average cost of $100/hour for an internal resource, the total maintenance cost of these ongoing activities can easily reach $4000.00/quarter. By comparison, a PolicyShield subscription for 2 organizational users costs $400/quarter.

5. Total Cost Savings Estimates

If we combine the cost savings of both policy development and maintenance, we see that a purchase of PolicyShield can save an organization over $8000.00 in initial development costs and over $14,000.00/year in ongoing maintenance if we assume an internal development cost of $100/hour.

Initial Development: $10,000.00 at $100/hour - $1600/year (Subscription)
Total Savings: $8400.00

Ongoing Maintenance: $16,000.00/year - $1600/year (Subscription)
Total Savings: $14,400.00/year

Summary

In even the most conservative estimates, PolicyShield 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/day, PolicyShield will pay back this initial price investment in two business days. After the initial investment in policy development, PolicyShield can pay for the monthly investment by saving only 1 hour of in-house development time per month.

Not only will information security policies based on PolicyShield 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.

6. References and Additional Resources

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

[2] ISO/IEC 17799:2005 (ISO 27002) – Code of practice for information security management - Published by ISO and available at BSI [http://www.bsi-global.org/]

[3] The Business Need for Updated Information Security Policies – Free Information Shield Whitepaper available at [http://www.informationshield.com]

[4] Information Security Roles and Responsibilities Made Easy, by Charles Cresson Wood - Published by Information Shield, Inc. [http://www.informationshield.com]