

# Cisco IP Communications Security

## Policy Development and Planning Guide

IP communications technology—the convergence of data, voice, and video onto a single network—offers enterprises attractive opportunities for reducing communication costs and complexities, as well as enabling dramatic increases in productivity, mobility, and resiliency. The key to unlocking the tremendous advantages of IP communications is helping ensure that the converged network—and all of its systems and services—is adequately protected.

Cisco Systems® offers integrated security solutions that provide the highest level of security protection available for your network, as well as IP communications and voice systems. Comprehensive security is achieved first by securing the network itself, and then by extending that security out to end stations and applications. Unlike solutions that only address point problems or products, the result is a thorough, layered approach that is unmatched in the security industry.

Critical to the success of IP communications security is adherence to a well-thought-out and comprehensive security policy. The security policy should enforce the planning, design, implementation, operation, and optimization (PDIOO) approach. The PDIOO approach is an ongoing process that results in continual monitoring and improvement of IP communications security. The security policy should specify plans for network security, network design details, network implementation and configuration, and

network operations and usage (see figure 1). The security policy should also specify the frequency of security policy updates.

The primary objective of this document is to help network planners and administrators develop a useful security policy that specifies an expectant loss value for each identified threat. This document uses a cost benefit or return on investment (ROI) approach toward the creation of a security policy. Only by comparing the benefit of a security solution with the cost of a security solution can cost-effective solutions be selected for inclusion in the security policy. This approach helps ensure the security policy is aligned with the organizational objective of profitability.

While this guide serves as a reference in the development of a solid security policy, in no way can it guarantee protection against every security exposure. Please note that no vendor, including Cisco®, can guarantee complete protection against every security threat. Many other sources for the development of a security policy exist. One reference in particular that is worth noting is RFC 2196, a document prepared by the IETF that provides additional background on security planning.–  
[\[http://www.ietf.org\]](http://www.ietf.org)

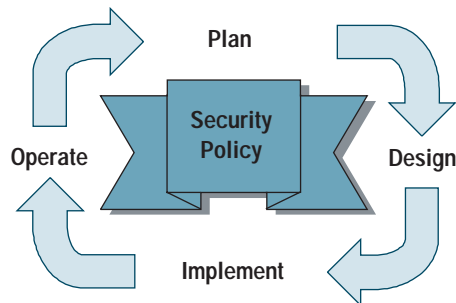


## Evaluating Risk

An underlying principle of the security policy is that it evaluates risk in relation to the organizational goal of profitability. A comprehensive security policy should take into consideration the expectant loss due to threats, and the solutions available to protect against those threats. Expectant losses can be both tangible and intangible. Replacement system costs, system recovery costs, and toll-fraud costs are examples of tangible costs that the company would incur in the event of a successful security attack. Loss of employee productivity and customer satisfaction are examples of intangible costs that the company would suffer (but not necessarily expense) due to a successful attack. When the cost of protecting against threats exceeds the expectant loss, the solution is said to have a negative return. A successful security policy attempts to define solutions that have a positive return.

While Cisco offers such technology solutions as firewalls, intrusion detection services (IDS), user authentication, and VPN to protect the network, other solutions not based on information technology, are also available for consideration. Physically securing computing solutions could be as inexpensive as the cost of a lock or key. Hiring security personnel is more expensive, but might be appropriate in certain situations. Installing video surveillance equipment or conducting employee background checks are solutions that could also have a positive return. First an analysis of the costs and benefits is needed to determine which solutions will provide a positive return. The most cost-effective solutions should then be documented in the security policy.

Figure 1  
The PDIOO Approach to Developing a Security Policy



Each step in the PDIOO process is not a discrete or independent step—they are all interrelated. The PDIOO process is also not a one-time event. Instead it is an iterative and on-going process. The planning stage consists of making decisions regarding the design, implementation, and operation of the network. A custom analysis of expectant losses and solution costs can help to identify the best security solutions. . It is important to note that different network designs can have on implementation and operational costs. Therefore, it is critical to s consider the design, implementation, and operational costs prior to beginning the planning process.

Conducting follow-up network security audits is an important part of the operations step. The frequency of these security audits is part of the planning step. As expectant losses due to threat changes and new threats begin to surface, new security solutions also become available, and existing solutions become more affordable. Analysis of the audit results, updated expectant loss computations, and updated security solution reviews help adjust the security policy with each round of planning. The result of each planning process is an appropriate update to the policy, which includes the timing of the next audit and security policy re-evaluation.



## The ROI of Protecting the Network

The primary objective of securing any communications network is to protect its availability, the privacy of data that it carries, and the integrity of this data. Achieving these objectives requires more than simply implementing a few standalone security devices and technologies. Instead, it demands a carefully developed security policy that specifies an appropriate security plan, design, implementation, and operations, with costs justified by the benefits.

Many security solutions and options exist today to aid in the protection of the network. The following are some examples of effective ways to help keep the network secure: using badges to access equipment rooms and locking systems with keys; maintaining redundant systems in separate buildings with backup power; configuring VLANs and deploying firewalls and VPNs; deploying intrusion detection and user authentication and authorization systems; restricting administrative privileges to only specified workstations or users and using one-time passwords; and, applying system patches and performing regular audits to the network.

The security options that any organization selects depends heavily on cost: how does the investment required to implement those options compare with the assessed risk exposure? Each security option can be viewed as an independent investment vehicle for which a cost justification or ROI analysis is needed. Only those options that yield a positive return should be considered for deployment.

## Annualized Loss Expectancy

The purpose of security solutions is to reduce the loss associated with threats. Annualizing this loss is suggested for ease of computing an ROI. Computing the annualized loss expectancy (ALE) begins with identifying the assets that a company is trying to protect and then identifying the threats to those assets.

Examples of assets to protect include:

- Hardware: Switches, routers, voice gateways, firewalls, IP phones, servers
- Software: Operating systems, database systems, source programs, utilities
- Data: Stored data, communication streams, audit logs, backups

Examples of possible threats worth protecting against include:

- Viruses, worms, and trojan horse attacks
- Denial-of-service attacks
- Eavesdropping on voice calls
- Impersonating another user's phone
- Toll fraud via unauthorized access
- Eavesdropping on voice-mail messages
- Stolen systems
- Loss of power
- System shutdown via command line
- System shutdown via power button

An ALE represents a monetary value for a particular threat against a particular asset. For example: What is the amount of loss associated with a worm infecting Cisco CallManager software? What is the amount of loss associated with the eavesdropping of a CEO's voice conversations? What is the amount of loss associated with unauthorized toll calls?



Computing ALE is not easy. Start by computing the single loss expectancy (SLE) of a particular threat against a particular asset. An asset is a network-based resource, process, application, or data from which an organization derives value. The asset is the target of a threat, and therefore requires protection. The SLE for a particular threat comprises a combination of many elements, such as: the replacement value of physical assets like hardware and software; lost revenue or sales; lost of employee productivity; damage to customer satisfaction, partner trust, and brand differentiation; and, additional organizational expenses, like inflated telecommunications charges from a toll fraud attack or the costs to get the network properly recovered after a threat. The duration of the impact and the number of users affected also significantly impacts the SLE, and therefore should be considered—as does the amount of built-in redundancy in place and the types of alternatives available in the event of an attack.

When a threat occurs, it does not necessarily cause a loss in all of the areas. For example, the SLE for theft of a redundant call-processing server includes the replacement value of the physical system and the cost of getting the replacement system operational. However, because the system is redundant, the SLE has no impact on revenues, employee productivity, or customer satisfaction. Conversely, the SLE for a virus or worm does not require the purchase of a replacement system, but likely incorporates losses in revenues, employee productivity, and customer satisfaction. The SLE for a virus also includes substantial costs for restoring all systems to normal operation.

There may be numerous closely related SLEs. For example, there might be SLEs for a range of virus attacks. Some virus attacks are very minor and cause little harm; others can be devastating. It is important to distinguish between the different types of threats and attacks and compute an SLE for each.

Once a company has determined the SLE for each possible type of attack, it must factor in the likelihood of occurrence to compute the ALE. For example, a particular type of virus attack might occur four times a year. Therefore, the ALE would be four times the SLE. Theft of a server might only happen once every three years. In this case, the ALE would be one-third the SLE. Computing the ALE is an important step to preparing accurate financial justifications for security solutions.

#### Comparing Expectant Loss to Security Solution Costs

After computing the ALE for a particular threat, it is important to compare it to the cost of the available security solution options. In order to determine this comparison, the following adjustment factors may be required to accurately calculate the ALE and solution cost.

The life expectancy of the solution should be factored into both the loss expectancy and the solution cost. For example, the installation of a new firewall provides protection for more than a single year. So, if a typical ROI justification looks at a three-year window, the cost of the firewall would have to be compared with three times the ALE associated with the threats the firewall would protect against. Any ongoing operational costs over the three-year period should also be added to the solution cost.

Many security options provide protection from multiple threats. Hence, the cost of a security solution must be allocated appropriately to all of the threats that it is meant to protect against. For example, a firewall not only helps to provide protection from denial-of-service attacks, it also provides protection from eavesdropping. Intrusion detection systems and software protect against many different types of threats and each threat should be individually assessed with its own ALE. In the case of multiple threats, the key to deciding what portion of the solution cost to use is to help ensure that the complete solution cost is accounted for, but never duplicated.



If a solution option only partly addresses a threat, then the ALE must be appropriately prorated. For example, if a new firewall protects against 90 percent of the denial-of-service attacks, and the ALE of a denial-of-service attack is US\$500,000, then the benefit received is only 90 percent of \$500,000, or \$450,000. In this case, it is the reduction in the ALE associated with a security solution that should be compared with the solution cost.

Implementation of one new security solution may make another security solution redundant and, therefore, allow its removal. The savings generated from removing the ongoing costs of an existing solution are always subtracted from the cost of the new solution.

After appropriately adjusting the loss expectancy and solution costs, compare the two. If the adjusted loss expectancy is greater than the solution cost, then a positive ROI exists for that solution. This represents a simple payback ROI approach; if needed, a more detailed analysis that factors in the time value of money can also be conducted.

### Security ROI Example

Consider the need to protect Cisco CallManager software from worms. The finalized SLE for this hypothetical example appears in Table 1:

Table 1 The SLE for Protecting Cisco CallManager from a Worm Attack

NEED TITLE	NEED TITLE
Loss of productivity to 200 employees due to 15 minutes of outage	\$15,000
Loss of revenues	–
Replacement cost of systems	–
Replacement cost of systems	–
Cost of worm cleanup	\$15,000
Impact to customer satisfaction	\$10,000
<b>Single Loss Expectancy</b>	<b>40,000</b>

The expectation is that the organization will face a worm attack 2.5 times a year, so the ALE for this example is \$100,000. In this example, the network security planners, designers, and administrators determined that a viable security solution would be to add a new firewall between the Cisco CallManager and all other systems. The finalized cost for the three-year life of this proposed solution is detailed in Table 2:

Table 2 The Finalized Security Solution Cost for Protecting Cisco CallManager from a Worm Attacks

NEED TITLE	NEED TITLE
Firewall cost	30,000
Initial implementation cost	10,000
3 yr equipment maintenance cost	3,000
3 yr administrative personnel cost	7,000



Table 2 The Finalized Security Solution Cost for Protecting Cisco CallManager from a Worm Attacks (Continued) (Continued)

NEED TITLE	NEED TITLE
Security Solution Cost	50,000

It is determine that this security solution will protect against 75 percent of the potential worm attacks that the organization could face. Therefore, the improved ALE for this security solution option is \$225,000 (or \$100,000 x 3 x .75). Firewall implementation is also deemed an effective means to aiding in the protection against unauthorized access to Cisco CallManager administration, which can be used to modify user permissions to allow for toll fraud. The prorated solution cost allocated to protecting against toll fraud is 25 percent, so the solution cost for addressing worms is \$37,500.

In this example, the organization agrees that investing \$37,500 is well worth protecting against an expected loss of \$225,000 due to worms. Therefore, implementation of a firewall between Cisco CallManager and all other systems is added to the security policy. While this example might seem trivial, it should give a sense of the process required to help ensure that network security objectives have a positive ROI.

#### Security Solutions

The following list of security options, while not exhaustive, provides solutions that Cisco feels are most worthy of consideration due to their strong ROI:

- VLAN segmentation
- Access control lists (ACLs)
- Application layer gateways/stateful firewalls
- Network intrusion detection system
- Host-based intrusion detection system
- Antivirus software (servers and desktops)
- Access control server/user authentication and authorization
- Dynamic Address Resolution Protocol (ARP) inspection
- IP source guard and Dynamic Host Configuration Protocol (DHCP) snooping
- Disable IP phone data port
- Switch port security

Some of these solutions are integrated features of Cisco solutions, limiting implementation costs only to provisioning and maintaining the feature. In addition to specific technology solutions, many network design, implementation, and operational choices can have a large impact on the cost effectiveness of increasing security. The predominant costs associated with these options are the changes in network implementation and operations.

The following is a list of technology-based solutions:

- VLAN segmentation
- Firewalls
- “Deny all” or “accept all” approach
- Network user authentication
- Password policy

- Disabling unused services on servers and network systems
- Disabling autoregistration
- Providing every 802.1q trunking port with a Port VLAN Identifier (PVID)
- RFC 1918 IP addresses
- Multilevel administration and authorization levels
- Dial plan restrictions
- Private LANs for network and system admin
- Log-in services to track access and configuration changes
- Frequent application of software patches and updates
- Regular audits
- Regular analysis and implementation of new security technologies
- Regular reviews and updates of security policy
- Frequently reviewing system logs
- Subscribing to security e-mail lists and bulletin boards
- Cross training on systems and regular training updates for administrators
- Publishing all user security guidelines and penalties

The following is a list of non-technology solutions:

- Cypher lock or keyed lock access to network and computing systems
- Badged access to network and computing systems
- Video surveillance of network and computing systems
- Video surveillance of external doors
- Security Guards
- Background checks on employees and administrators
- System level key locks

## Summary

A security policy has many components and this guide has not attempted to touch on all of them. Nor has this document attempted to make any recommendations as to which security solutions are best for a particular organization. The primary objective of this document is to position the ongoing PDIOO process as an effective way to help ensure that the components of the security policy are consistently evaluated for positive ROI. Secondary objectives are to identify: the most serious threats to an IP communications network, the major determinants to calculating loss expectancy resulting from a threat, and the predominant solutions available to address those threats.

Cisco offers additional best practice documentation including design guides, implementation guides, and operations guides to assist planners, analysts, and administrators by providing more details on the specific solutions available and the considerations for implementing those solutions.

For additional information on the Cisco IP Communications Security Solution, visit

[http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking\\_solutions\\_package.html](http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_package.html)



### Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

### European Headquarters

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

### Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

### Asia Pacific Headquarters

Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)  
ETMG 203246—CM 02.04