Planning Report 02-1

The Economic Impact of Role-Based Access Contro

Prepared by:
RTI
for

National Institute of Standards & Technology

Program Office
Strategic Planning and
Economic Analysis Group

March 2002

U.S Department of Commerce
Technology Administration

The Economic Impact of Role-Based Access Control

Final Report

SUBMITTED TO:

Gregory Tassey, Ph.D.
National Institute of Standards and Technology
Acquisition and Assistance Division
Building 101, Room A1000
Gaithersburg, MD 20899-0001

SUBMITTED BY:

Michael P. Gallaher, Ph.D.
Alan C. O'Connor, B.A.
Brian Kropp, Ph.D.
RTI
3040 Cornwallis Road
P.O. Box 12194
Research Triangle Park, NC 27709-2194

RTI Project Number 07007.012

March 2002

RTI INTERNATIONAL

The Economic Impact of Role-Based Access Control

Final Report

March 2002

SUBMITTED TO:

Gregory Tassey, Ph.D.
National Institute of Standards and Technology
Acquisition and Assistance Division
Building 101, Room A1000
Gaithersburg, MD 20899-0001

SUBMITTED BY:

Michael P. Gallaher, Ph.D.
Alan C. O'Connor, B.A.
Brian Kropp, Ph.D.
RTI
Health, Social, and Economics Research
Research Triangle Park, NC 27709

RTI Project Number: 07007.012

Contents

Figures

Tables

Executive Summary

Information technology has enabled U.S. businesses to improve their employees' productivity, integrate their supply chains, and automate and improve their interactions with customers. Increasingly, more functions, including inventory management, invoice payments, and customer support, are handled over intranets and the Internet.

As organizations increase the functionality and information offered on internal and external networks, controlling access to information and other resources becomes more complex and costly. In addition, security failures can disrupt an organization's operations and can have financial, legal, human safety, personal privacy, and public confidence impacts.

This study quantifies the benefits of role-based access control (RBAC) and estimates NIST's impact on the development and adoption of RBAC.

Access control systems within a computer network are used to control the actions, functions, applications, and operations of legitimate users within an organization and to protect the integrity of the information stored within the system. Role-based access control (RBAC) is a relatively new access control system that maps to organizational-specific structures in a way that reduces direct and indirect administrative costs and improves security.

The National Institute of Standards and Technology (NIST) began working on RBAC in the early 1990s after a study of federal agency security needs identified the need to develop a better method for managing large networked systems and complex access issues (Ferraiolo, Gilbert, and Lynch, 1992). Over the past decade, NIST's RBAC project has made significant contributions to the development and adoption of RBAC through publishing in the

professional literature, sponsoring conferences and outreach projects, and supplying infrastructure tools to industry.

The objectives of this study was to conduct a microeconomics impact assessment of the

- benefits of RBAC relative to alternative access control systems, and
- economic return from the NIST/Information Technology Laboratory (ITL) RBAC project's contributions to the development and adoption of RBAC.

Based on interviews with software developers and companies using RBAC-enabled products, we projected that the net present value of RBAC through 2006 will be approximately $671 million. NIST's contributions were estimated to account for 44 percent of the benefits of RBAC, leading to a social rate of return to the NIST/RBAC project of approximately 62 percent.

ES.1 OVERVIEW OF RBAC

Although role-based security models have existed for 20 years, their application has until recently been limited. To date, most systems have based access control on the discretion of the owner or administrator of the data as opposed to basing access on the often nondiscretionary organization-wide policies as is done with RBAC. These owner-controlled systems worked adequately for small local area networks (LAN) but have become cumbersome to manage and error prone as networking capabilities have increased.

RBAC allows companies to specify and enforce security policies that map naturally to the organization's structure.

RBAC is a technology that offers an alternative to traditional discretionary access control (DAC) and mandatory access control (MAC) policies. RBAC allows companies to specify and enforce security policies that map naturally to the organization's structure. That is, the natural method for assigning access to information in a company is based on the individual's need for the information, which is a function of their job or role within the organization. RBAC allows a security administrator to use the natural structure of the organization to implement and enforce security policy. This technology decreases the cost of network administration while improving the enforcement of network security policies.

ES.2 NIST'S CONTIBUIONS TO RBAC

One software company stated that "…NIST's contribution was critical in establishing a taxonomy and a shared vocabulary for us, our customers and the industry as a whole."

NIST's RBAC project responded to a demonstrated need for improved security mechanisms and the related standards to support the development and adoption of new complex networked security systems. At that time industry believed that a lack of standardization was hampering the development of appropriate access control products, and that a key to the success of such a system would be its ability to operate across a wide range of operating systems (Ferraiolo, Gilbert, and Lynch, 1992).

In 1992 NIST published the first comprehensive RBAC model. Although the concept of roles has been used in software application and mainframe environments for at least 25 years, it has only been within the last decade that RBAC has emerged as a full-fledged model as mature as traditional mandatory and discretionary access control concepts. The roots of NIST's early RBAC model included the use of groups in UNIX and other operating systems, privilege groupings in database management systems, and separation of duty concepts described in early papers. The modern concept of RBAC as used within the research community and implemented within a growing number of commercial implementation originates from this early work. The impact of this work includes the ability to specify and enforce a wider range of access control policies, thereby reducing the number of illicit user accesses as well increasing administrative and end-user productivity.

NIST's RBAC project has accelerated the introduction and acceptance of RBAC-based products in the marketplace. In addition, NIST's contributions have reduced the cost of R&D for private companies developing network security products based on RBAC.

NIST's contributions range from developing and formalizing the fundamental concepts of RBAC models to demonstrating their capabilities and providing implementation tools to industry. These contributions can be grouped into two general categories:

- the development of generic technologies that provide the technology base for RBAC market applications, and
- the development of infratechnologies that support implementation and interoperability across different systems.

Generic technologies provide the technology base from which market applications are derived (Tassey, 1997).

NIST developed the technical specifications and formal description of the RBAC model (Ferraiolo and Kuhn, 1992). Since the first formal specification, NIST has expanded its model by incorporating different types of role relationships. The papers NIST has published and the patents it has received have been widely cited by academics and have provided the technology base for many of the commercial products being introduced by software vendors. In addition, NIST has co-founded a series of ACM workshops on RBAC through which close to 100 papers from sources all over the world have been published. This workshop series has evolved into the present ACM Symposium on Access Control Models and Technology now in its 7th year.

Infratechnologies are a set of "technical tools" that include scientific and engineering data, measurement and test methods, and practices and techniques that are widely used in industry (Tassey, 1997).

NIST has also developed specific tools for implementing RBAC for the World Wide Web (Barkley et al., 1997). The tools NIST has developed to assist in implementing RBAC Web include RGP-Admin, a tool for managing role/permission relationships, and AccesMgr, a graphical user interface for managing access control lists for Windows NT files. NIST has demonstrated the use of RBAC for the Web for corporate intranets (Ferraiolo, Barkley, and Kuhn, 1999) and for the health care industry (Barkley, 1995) and has implemented RBAC on the NSA Synergy secure operating system.

NIST has developed the Role Control Center as a reference implementation and a demonstration platform for the viability of advanced RBAC concepts. The center disseminates information on concepts ranging from multiple inheritance hierarchies, to the enforcement of a variety of separation of duty policies across multiple heterogeneous servers and applications.

NIST, in conjunction with Ravi Sanhdu and Serban Gavrila, has also proposed a standard for RBAC. The standard is intended to reduce the uncertainty and confusion about RBAC's utility and meaning and to serve as a foundation for product development, evaluation, and procurement specifications (Ferraiolo, 2001).

ES.3 ESTIMATING THE BENEFITS OF RBAC

To estimate the benefits of RBAC we conducted telephone interviews and Internet surveys with software developers and organizations (referred to as end users) that integrate RBAC products into their business operations. In addition, a case study

was conducted with a multi-product insurance company. The information collected was used to quantify the benefits and costs per employee managed by RBAC systems.

The growth of employees managed using RBAC systems was projected through the year 2006. It is estimated that by 2006 between 30 and 50 percent of employees in the service sector and between 10 and 25 percent of employees in nonservice sectors will be managed by RBAC systems. Because of the uncertainty surrounding the penetration estimates, high, medium and low penetration scenarios were estimated. The remainder of this executive summary refers to the medium penetration scenario.

RBAC administrative and productivity benefits lead to an annual operating benefit of $43.71 per employee. This leads to a net benefit through the year 2006 of $671 million.

Technical and economic metrics for RBAC's impact on end users were developed for the Internet surveys. Key impact metrics are administrative savings associated with managing access to information systems and reduced employee downtime from waiting to receive system access. These RBAC systems administrative and productivity benefits lead to an annual operating benefit of $43.71 per employee.

However, the benefit of RBAC will not be realized without costs. Software developers indicated that on average they incurred $550,000 in R&D expenditures to develop RBAC-enabled products. In addition, based on our in-depth case study with a multiproduct financial services firm, the average end-user customization and implementation costs are estimated to be $78.36 per employee. These costs are incurred once per employee.

Table ES-1 summarizes the benefits and costs associated with RBAC. The NPV of net benefits (benefits less costs) through 2006 are $671.1 million. Costs are expressed as negative benefits.

ES.4 MEASURES OF ECONOMIC RETURN TO THE NIST/RBAC PROJECT

"The NIST implementation was a groundbreaking and significant contribution to software technology."

Based on interviews with software developers and end users of RBAC products, it was estimated that the activities of the NIST/RBAC project

- ➤ accelerated the development and adoption of RBAC by 1 year and

Table ES-1. NPV of Benefits and Costs of RBAC through 2006

	NPV through 2006 ($2000)
R&D expenditures: software developers and in-house development	–53.2
End-users' customization and implementation costs	–161.7
End-users' operation benefits	886.0
Net benefits of RBAC	671.1

- lowered research and development costs for software vendors by approximately 6 percent.

Using this information we construct two times series that show the net benefits of RBAC with and without NIST's contributions. The difference between the with and without NIST time series is the economic impact of the NIST/RBAC project (i.e., it is the change in net benefits attributable to NIST). As shown in Table ES-2, the net present value of NIST's impact on the benefits of RBAC is $295 million under the medium penetration scenario.

Table ES-2. Time Series of the Net Benefits of RBAC With and Without NIST's Contributions ($millions)[a]

Year	Baseline (with NIST)	Counterfactual (without NIST)	Total Change in Net Benefits (ΔNB_t)
1992	—	—	—
1993	—	—	—
1994	—	—	—
1995	—	—	—
1996	–5.05	—	–5.05
1997	–5.05	–5.50	0.45
1998	–5.05	–5.50	0.45
1999	–5.05	–5.50	0.45
2000	–18.08	–5.50	–12.58
2001	–0.36	–16.90	16.54
2002	19.84	–0.33	20.17
2003	60.26	18.54	41.72
2004	207.08	56.32	150.76
2005	308.51	193.53	114.97
2006	337.85	288.33	49.52
NPV (2000)	671.08	376.31	294.77

[a]All numbers have been adjusted to 2000 dollars.

"This is probably one of the best examples of how an organization like NIST can help the private sector. The existence of a widely visible prototype advanced the concrete understanding of corporate IT architects so significantly that we were able to get unusually good early feedback validating and influencing our design choices."

We used NIST's expenditures and their related impact on the net benefits of RBAC to calculate a NPV, benefit-cost ratio, and an internal rate of return (IRR) for the NIST/RBAC project. These three measures of economic return are presented in Table ES-3. The measures are shown for the high, medium, and low penetration scenarios. The NPV of NIST's impact under the medium penetration scenario is $294.8 million. The benefit-cost ratio ranges from 69 to 158, and the IRR ranges from 39 to 90 percent.

The impacts of NIST's RBAC project quantified in Table ES-2 and Table ES-3 include only the administrative and productivity benefits. They do not reflect the potential security benefits associated with RBAC. Most companies interviewed indicated that RBAC would reduce the frequency and severity of security violations. However, because this information is highly sensitive, this study was not able to quantify the benefit of improved system security. For this reason the impact estimates presented above are conservative and should be considered lower-bound estimates of the benefits of RBAC and the economic return from the NIST/RBAC project.

Table ES-3. Measures of Economic Return to the NIST/ITL RBAC Project ($millions)[a]

	High	Medium	Low
a. NPV change in net benefits	427.42	294.77	185.71
b. NPV NIST expenditure	2.70	2.70	2.70
NPV of the NIST/ITL RBAC project (a – b)	425	292	183
Benefit-cost ratio	158	109	69
Internal rate of return	90%	62%	39%

[a]All numbers have been adjusted to 2000 dollars.

1 Introduction

The National Institute of Standards and Technology (NIST) began working on role-based access control (RBAC) in the early 1990s after a study of federal agency security needs identified the need to develop a better method for managing large networked systems and complex access issues (Ferraiolo, Gilbert, and Lynch, 1992). The objective of this study is to conduct a microeconomics impact assessment of the NIST/Information Technology Laboratory (ITL) RBAC project.

This section discusses some of the trends in computer applications and security needs, provides an overview of NIST's role in developing RBAC, and outlines the approach used to estimate the economic impact of the NIST/ITL RBAC project.

1.1 TRENDS IN COMPUTER APPLICATIONS AND SECURITY NEEDS

Information technology has enabled U.S. businesses to improve their employees' productivity, integrate their supply chains, and automate and improve their interactions with customers. The use of external web sites for marketing and recruiting is common, and internal corporate intranets provide employees and suppliers easy access to organizational resources and information. Increasingly, more functions, including inventory management, invoice payments, and customer support, are handled over intranets and the Internet, regardless of the underlying information technology infrastructure (Barkley et al., 1997).

As organizations increase the functionality and information offered on internal and external networks, controlling access to information and other resources becomes more important and complex. Organizations must develop and enforce access policies that protect sensitive and confidential information; prevent conflict of interest; and protect the system and its contents from intentional and unintentional damage, theft, and unauthorized disclosure. Security failures can disrupt an organization's operations and can have financial, legal, human safety, personal privacy, and public confidence impacts (Ferraiolo, Gilbert, and Lynch, 1992).

Safeguarding information resources can be very complicated and expensive. Network administrators must maintain access control lists that specify the resources each user is allowed to access. They must issue passwords and permissions to enforce the access lists and update them as personnel change and as users' needs and permissions change. Maintaining access while enforcing a comprehensive, coherent security policy has become an expensive and complex undertaking. Simplifying it could have an important impact on the cost and effectiveness of electronic resource access policies.

RBAC is a technology that offers an alternative to traditional discretionary access control (DAC) and mandatory access control (MAC) policies. RBAC allows companies to specify and enforce security policies that map naturally to the organization's structure. That is, the natural method for assigning access to information in a company is based on the individual's need for the information, which is a function of his job, or role, within the organization. RBAC allows a security administrator to use the natural structure of the organization to implement and enforce security policy. This technology decreases the cost of network administration while improving the enforcement of network security policies.

1.2 NIST'S CONTRIBUTIONS TO RBAC

NIST's RBAC project responded to a demonstrated need for improved security mechanisms and the related standards to support the development and adoption of new complex networked security systems. At that time industry believed that a lack of standardization was hampering the development of appropriate

access control products, and that a key to the success of such a system would be its ability to operate across a wide range of operating systems (Ferraiolo, Gilbert, and Lynch, 1992).

Public funding is frequently used to support the development of generic technologies and infratechnologies because these technologies possess many of the characteristics of a public good. Public goods, unlike private goods, are typically underprovided by private markets as compared to their socially optimal levels of provision (Stiglitz, 1988).

In 1992 NIST published the first comprehensive RBAC model. Although the concept of roles has been used in software application and mainframe environments for at least 25 years, it has only been within the last decade that RBAC has emerged as a full-fledged model as mature as traditional mandatory and discretionary access control concepts. The roots of NIST's early RBAC model included the use of groups in UNIX and other operating systems, privilege groupings in database management systems, and separation of duty concepts described in early papers. The modern concept of RBAC as used within the research community and implemented within a growing number of commercial implementation originates from this early work. The impact of this work includes the ability to specify and enforce a wider range of access control policies, thereby reducing the number of illicit user accesses as well increasing administrative and end-user productivity.

NIST's RBAC project has accelerated the introduction and acceptance of RBAC-based products in the marketplace. In addition, NIST's contributions have reduced the cost of R&D for private companies developing network security products based on RBAC.

NIST's contributions range from developing and formalizing the fundamental concepts of RBAC models to demonstrating their capabilities and providing implementation tools to industry. Table 1-1 provides an overview of NIST's RBAC activities. These contributions can be grouped into two general categories:

- the development of generic technologies that provide the technology base for RBAC market applications, and
- the development of infratechnologies that support implementation and interoperability across different systems.

1.2.1 Generic Technologies

NIST developed the technical specifications and formal description of the RBAC model (Ferraiolo and Kuhn, 1992). Since the first formal specification, NIST has expanded its model by incorporating

Table 1-1. Overview of NIST's RBAC Activities
NIST's contributions range from developing and formalizing the fundamental concepts of RBAC models to demonstrating their capabilities and providing implementation tools to industry.

Category	Activities
Patents	Implementation of Role Based Access Control in Multi-level Secure Systems (Kuhn). U.S. Patent #6,023,765
	Workflow Management Employing Role-Based Access Control (Barkley). U.S. Patent #6,088,679
	A Method for Visualizing and Managing Role-Based Policies on Identity-Based Systems (Ferraiolo and Gavrila) (pending)
	Implementation of Role/Group Permission Association Using Object Access Type (Barkley, Cincotta). U.S. Patent #6,202,066
Papers	"Role Based Access Control: Features and Motivations" (Ferraiolo, Cugini, Kuhn, 1995), Computer Security Applications Conference
	"Mutual Exclusion of Roles as a Means of Implementing Separation of Duty in Role-Based Access Control Systems" (Kuhn, 1997), Second ACM Workshop on Role-Based Access Control
	"Implementing Role Based Access Control Using Object Technology" (Barkley, 1995), First ACM Workshop on Role-Based Access Control
	"Role-Based Access Control for the Web" (Barkley, Kuhn, Rosenthal, Skall, Cincotta, 1998), CALS Expo International & 21st Century Commerce 1998: Global Business Solutions for the New Millennium
	"Specifying and Managing Role-Based Access Control within a Corporate Intranet" (Ferraiolo, Barkley, 1997), Second ACM Workshop on Role-Based Access Control
	"Role Based Access Control for the World Wide Web" (Barkley, Cincotta, Ferraiolo, Gavrila, Kuhn, 1997), 20th National Computer Security Conference
Conferences	ACM workshop on RBAC
	RBAC demonstrations
Standards Development	A Proposed Standard for Role-Based Access Control (Ferraiolo et al., 2001)
Web Tools and Software	RBAC for UNIX/POSIX/LINUX
	RBAC for Windows NT
	RGP-Admin
	AccesMgr
Industry Outreach Projects	RBAC for Synergy
	RBAC Small Business Innovation Research (RBAC SBIR)
	RBAC for the World Wide Web (RBAC/Web)
	Role Control Center

different types of role relationships (Kuhn, 1997; Gavrila and Barkley, 1998; Barkley and Cincotta, 1998).

Generic technologies provide the technology base from which market applications are derived (Tassey, 1997).

The papers NIST has published and the patents it has received have been widely cited by academics and have provided the technology base for many of the commercial products being introduced by software vendors. NIST has presented its work at a number of professional conferences and has co-founded a series of Association for Computing Machinery (ACM) workshops on RBAC. Now in its seventh year, this workshop series has published close to 100 papers from sources all over the world. NIST has received two patents for its RBAC models and has applications pending for two more.

Most of the companies interviewed indicated that they would not have pursued the development of these generic technologies on their own. Thus, by demonstrating the technical feasibility of RBAC through its publications and conferences, NIST has reduced development uncertainty and provided the technology base to accelerate the introduction of RBAC features into commercial access control systems.

1.2.2 Infratechnologies

NIST has developed specific tools for implementing RBAC for the World Wide Web (Barkley et al., 1997). The tools NIST has developed to assist in implementing RBAC Web include RGP-Admin, a tool for managing role/permission relationships, and AccesMgr, a graphical user interface for managing access control lists for Windows NT files. NIST has demonstrated the use of RBAC for the Web, for corporate intranets (Ferraiolo, Barkley, and Kuhn, 1999), and for the health care industry (Barkley, 1995) and has implemented RBAC on the NSA Synergy secure operating system.

Infratechnologies are a set of "technical tools" that include scientific and engineering data, measurement and test methods, and practices and techniques that are widely used in industry (Tassey, 1997).

NIST, in conjunction with Ravi Sanhdu and Serban Gavrila, has also proposed a standard for RBAC. The standard is intended to reduce the uncertainty and confusion about RBAC's utility and meaning and to serve as a foundation for product development, evaluation, and procurement specifications (Ferraiolo et al., 2001).

NIST has developed the Role Control Center as a reference implementation and a demonstration platform for the viability of advanced RBAC concepts. The center disseminates information on

concepts ranging from multiple inheritance hierarchies, to the enforcement of a variety of separation of duty policies across multiple heterogeneous servers and applications.

NIST's role in developing RBAC infratechnologies has been important because these technology tools cannot easily be embodied in commercial products or processes. As a result, the private sector has difficulty appropriating returns from the development of infratechnologies. This market failure typically leads to an underinvestment in infratechnologies in the absence of government support.

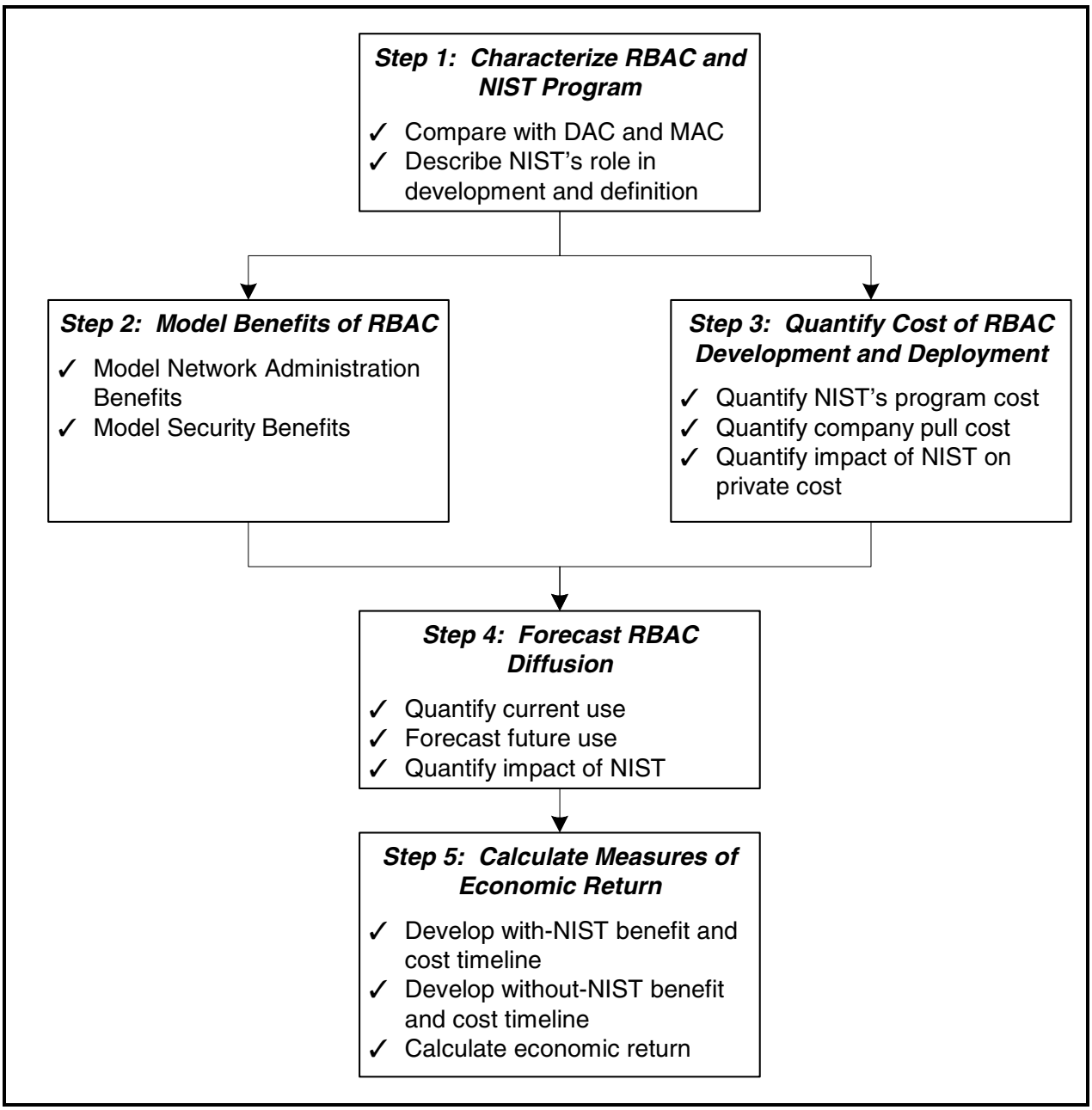
1.3 OVERVIEW OF APPROACH TO MEASURE THE ECONOMIC IMPACT OF NIST'S RBAC PROJECT

The approach to measure the economic impact of NIST's RBAC project consists of the five steps shown in Figure 1-1. The first step (discussed in Section 2) compared the technical specifications of the RBAC model with other methods for access control. This comparison provided the input needed for modeling the incremental benefits of RBAC. The analysis also included a detailed description of NIST's role in developing and defining RBAC and the market failures that led to underinvestment by industry. Information was obtained from interviews with industry experts throughout the supply chain and from academic and industry publications.

In the next step (presented in Section 3) we developed a detailed model of the incremental benefits of RBAC relative to the other access control methods. The model captures the benefits of RBAC's simplification of network administration and defines metrics for quantifying these benefits. RBAC's potential benefits of increasing the effectiveness of network security policy are included in the theoretical model even though empirical data on these benefits are limited.

Step 3 required that we quantify the benefits and cost of RBAC development and deployment. Section 4 describes the surveys and case studies used to obtain the data and presents the quantified benefit and cost impact metrics we used to estimate economic

Figure 1-1. Approach to Estimating the Economic Returns from NIST's RBAC Project
Our approach involved developing a baseline and two counterfactual scenarios.



impacts. Costs include NIST's program costs, the cost to developers of computer programs that incorporate RBAC, and the cost to companies that purchase and use RBAC-based tools.

In Step 4 we forecasted the diffusion of RBAC technology with and without the NIST RBAC project. This forecast was used in Step 5 to

develop timelines of the costs and benefits of the RBAC project, and we used these timelines to estimate the return to NIST's investment. This step captures NIST's impact on the timing of RBAC development and the speed and extent of its diffusion.

2 The Evolution of RBAC

RBAC has emerged as a viable alternative to traditional access control policies, such as DAC and MAC, because it is based on an enterprise's organizational structure. As such, systems, data, and applications administrators and owners can more effectively manage and maintain information resources in a manner consistent with enterprise-wide security policies. RBAC has the further benefit of facilitating systems administration by assigning roles to manage users as opposed to using each individual user's identity to manage users.

Although role-based security models have existed for 20 years, their application has until recently been limited. To date, most systems have based access control on the discretion of the owner or administrator of the data as opposed to basing access on organizational or policy needs as is done with RBAC. These owner-controlled systems worked adequately for small local area networks (LAN) but have become cumbersome to manage and error prone as networking capabilities have increased. The explosion of electronic data exchange and interconnection of information systems led to significant productivity gains in the 1990s. However, these same factors have also increased electronic security and integrity concerns. Confidentiality restriction and regulatory requirements have caused organizations to look for improved approaches to manage the types of users that may have access to which data and to which applications. The result is a renewed and growing interest in role-based security models.

Several organizations, including NIST, have been working since the early 1990s to define a common standard for RBAC and to spur its implementation by providing research and development support to this emerging technology. Although relatively few software companies currently market RBAC and RBAC-enabled products, the market for these products is expected to grow rapidly in the near future.

This section provides background information needed to understand RBAC in the context of the marketplace, including RBAC's benefits and the barriers to its adoption. The following issues are discussed:

- technical characteristics and underlying concepts of RBAC, including a comparison of RBAC to defender access control models;
- benefits of RBAC, particularly those related to administering computer networks, both within an organization and its extranet;
- RBAC industry supply chain, including information on the software developers who supply RBAC-enabled software and the characteristics of end users who purchase this software;
- barriers software developers face when developing and integrating RBAC models into their products;
- barriers software end users face in implementing RBAC; and
- NIST's contribution to the development and deployment of RBAC and the mitigation of market barriers.

2.1 RBAC TECHNICAL CHARACTERISTICS

Access control is generally concerned with determining what users and groups of users can perform what operations on what resources. The fundamental problem is that each system and application for which access control is enforced has a proprietary method for creating and managing users, groups, and a system-specific meaning of operations and objects. For many organizations, the number of systems can be in the hundreds or even thousands, the number of users can range from the hundreds to the hundreds of thousands, and the number of resources that must be protected can easily exceed a million.

How does RBAC help? RBAC is designed to centrally manage privileges by providing layers of abstractions that are mapped one-

to-many to real users and real operations and real resources. Managing permissions in terms of the abstractions reduces complexity and provides visualization and a context for implementing complex access control policies. Abstractions can be centrally managed resulting in real permissions on real systems.

In taking advantage of these abstractions RBAC offers greater administrative efficiency as well as the ability to intuitively administer and enforce a wide range of access control policies. In RBAC, permissions are associated with roles, and users are made members of roles, thereby acquiring the role's permissions. The implementation of this basic concept has been shown to greatly simplify access control management. Roles are centrally created for the various job functions in an organization, and users are assigned roles based on their responsibilities and qualifications. As such, users can be easily reassigned from one role to another. Users can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed. For example, if a user moves to a new function within the organization, the user can simply be assigned to the new role and removed from the old one, whereas in the absence of RBAC, the user's old privileges would have to be individually located, revoked, and new privileges would have to be granted.

To provide further administrative efficiency, RBAC allows roles to inherit other roles and as such form role hierarchies. For example, the role "cardiologist" is hierarchically superior to the role "doctor," if the cardiologist has (inherits) all of the privileges of the doctor, and the users that are authorized for the "cardiologist" role are also authorized for the "doctor" role.

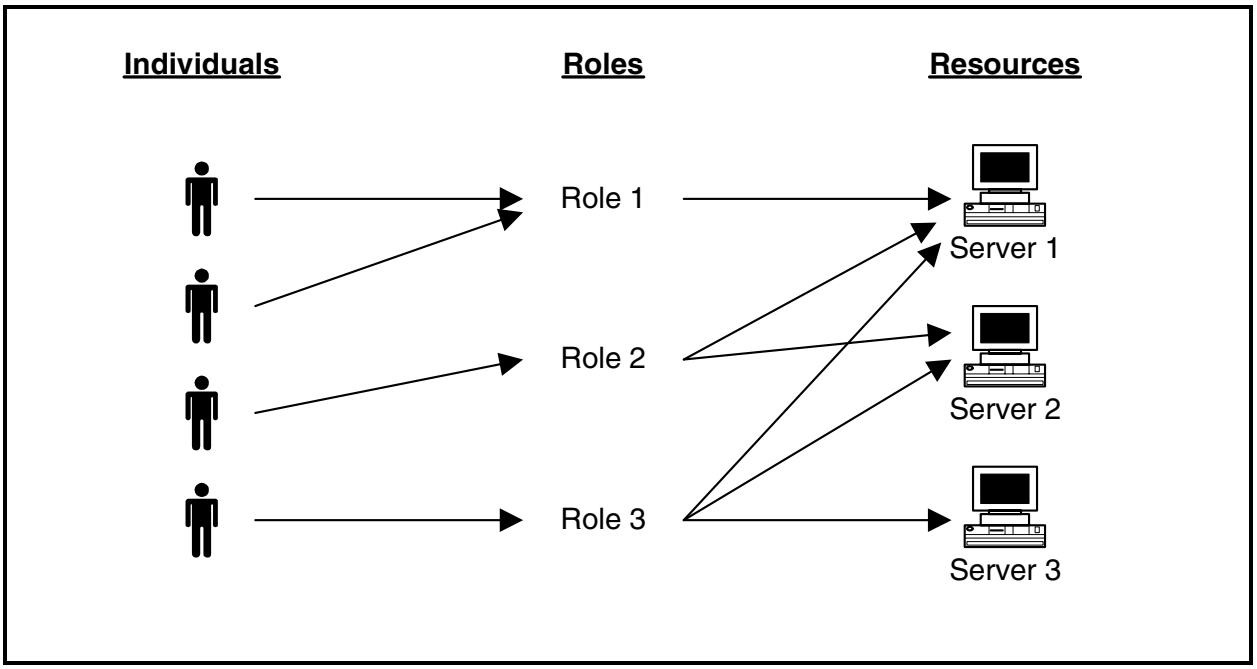
RBAC provides the capability to visualize and manage user privileges across heterogonous platforms and applications. By centrally storing and managing roles as both collections of users and collections of privileges, RBAC is able to define, constrain, review, and enforce access control policies as user/role, role/role, or role/privilege relations. RBAC is considered to be policy-neutral in the sense that, by using role hierarchies and constraints, a wide range of security policies can be expressed to include traditional DAC as well as a variety of nondiscretionary separation of duty (SOD) policies through the definition of constraints.

This remainder of section provides more details on the interaction among roles, users, and permissions. It also discusses the RBAC models that have been developed and compares them to alternative access control models, such as access control lists and MAC.

2.1.1 Users, Roles, and Permissions

Traditionally, the prevalent approach to granting access to information within a particular database or access to a particular application is to establish specific permissions for each user within an organization. If the user must have access to multiple applications and databases, the user must be assigned permissions for each resource. This approach is problematic for several reasons. When users enter, leave, or change responsibilities within an organization, updating the permissions of each user is difficult, time consuming, and possibly error-prone (Barkley and Cincotta, 1998). In addition, this approach leads to potential violations of information and system security. RBAC avoids these problems because it uses the user's role as the key to access rather than the user's identification (see Figure 2-1).

Figure 2-1. Role-Based Access Control



In a role-based model, each user may be assigned to multiple roles, and each role may have multiple users. The roles that users are assigned depend on their job responsibilities, and each role is assigned permissions. Permissions determine the data and applications that may be accessed and each role is assigned the set of permissions that are necessary for the user to perform his required tasks. Users' roles can pertain to specific jobs (bank teller, bank manager), geographic locations (New York, Chicago), or individual descriptors (trainee, shift supervisor). In most situations, users within the organization change more frequently than the roles or job functions within the organization. By associating roles with permissions and changing the users within the roles, administrative expenses decrease. If an organization experiences a significant amount of worker turnover relative to role turnover, RBAC can provide significant cost savings (Ferraiolo and Kuhn, 1992).

In most situations, users within the organization change more frequently than the roles or job functions within the organization. By associating roles with permissions and changing the users within the roles, administrative expenses are decreased.

Least Privilege

Roles improve security within a network by using the principle of least privilege. When a role is created within an organization, the user's level of access to information needs to be determined. Least privilege means that once access requirements are determined, that role should only be given permissions to accomplish the required tasks; no additional permissions should be given. In networks without role-based policies, users often have access permissions exceeding what is necessary. Where job responsibilities overlap job categories, administrators may be unable to limit access to sensitive information. RBAC improves security within the network because it prevents users from having access to information outside of their roles. This denial of access prevents users from circumventing the security policy within the network.

Separation of Duties

Within a larger task that the organization must accomplish, several subtasks may need to be performed. Because the subtasks may be separated into different roles, it is extremely difficult for a single individual to engage in fraud against the organization. The most common example of separation of duties is the separate subtasks involved in authorizing a payment for a particular transaction. By separating submission for payment and authorization for payment into separate roles, no individual can accomplish both tasks. This

mutually exclusive separation reduces the possibility of fraud within the organization. The specific separation of duties depends on the nature of the tasks and subtasks that the firm must accomplish. In some cases, the complete separation of tasks (submission and authorization) may be too difficult. Thus, the security advantage is outweighed by the additional transactions cost of accomplishing the task. In these cases, a more dynamic separation of duties could occur where the permissions within the role allow for submission and authorization. However, the same user cannot submit and authorize the same payment. A cross-check of user and role within the same task could be added to the system to accomplish the desired task (Ferraiolo and Kuhn, 1992).

2.1.2 RBAC Models and Evolution

The benefit of using roles to manage permissions is not a new concept, but the actual use of roles in network administration policy is new. A consensus has yet to emerge within the computer network and security community on what RBAC means, although role-based security models have been in existence for nearly 20 years. As a result, the spectrum of RBAC definitions includes models that range from the simple to the sophisticated. Sandhu (1998) and Sandhu et al. (1997) analyze the various definitions of RBAC. They define the basic RBAC model, referred to as $RBAC_0$, as including least privileges and separation of duties. Subsequent RBAC models build on this basic model, introducing new concepts of hierarchies and constraints that enhance administrative and security benefits (see Figure 2-2).

Figure 2-2. RBAC Definitions
As RBAC models have progressed, they have incorporated additional functionality.

Models	Hierarchies	Constraints
$RBAC_0$	No	No
$RBAC_1$	Yes	No
$RBAC_2$	No	Yes
$RBAC_3$	Yes	Yes

Note: All RBAC models include hierarchies and constraints.

RBAC$_1$

RBAC$_1$ is based on RBAC$_0$ and introduces the concept of **role hierarchies**. Role hierarchies are a natural extension of the authority and responsibility roles that exist within an organization. For example, an organization may have junior and senior roles. When role hierarchies are introduced, the senior role (e.g., bank president) has access to all of the information that the junior role (e.g., bank teller) has access to, but not vice versa.

This approach can increase the administrative efficiency of the network. Rather than respecifying all of the permissions of the junior role for the senior role, the junior role is specified as a permission of the senior role. As the levels of the organization or the numbers of permissions increase, the greater the benefit from establishing role hierarchies.

RBAC$_2$

RBAC$_2$ is also based on the original RBAC$_0$ model but introduces the concept of **constraints**. The most frequent use of constraints is to achieve separation of duties within an organization. For example, a constraint can state that if a user has a particular role, that user cannot be assigned a separate role. However, constraints can also be used in many other situations. Constraints can be used to establish membership to a particular role. If an organization wants to have only one department head, then it can impose a particular constraint stating that if someone is in a particular role, then no one else can be admitted to that role. This concept has been referred to as cardinality. Constraints can also be used as prerequisites for entry into roles. For example, the only way that role *x* can be assigned to a user is if the user is already in role *y*.

Interviews with software developers indicate that RBAC$_2$ and RBAC$_3$ models are not widely adopted in software products. The concensus is that although these models are likely to be adopted at some point in the future, the cost of their incorporation at present outweighs the additional product benefits. The additional functionality associated with these two RBAC models can be built into RBAC$_0$ and RBAC$_1$ through the role engineering process.

RBAC$_3$

The NIST RBAC model is RBAC$_3$. It is the most complex RBAC model, including both role hierarchies and constraints. In RBAC$_3$, constraints can be imposed on the hierarchical roles within an organization. For example, junior roles can be constrained to have a maximum number of senior roles, multiple junior roles can be constrained to have different senior roles, or constraints can be imposed on users to limit the number of senior roles to which they can be assigned. The sensitive interactions that occur between role

hierarchies and constraints in $RBAC_3$ make it the most sophisticated and complex RBAC model.

2.1.3 Alternative Access Control Technologies

In addition to role-based models, several competing technologies are used to address these needs. Whereas RBAC determines access to data based on organizational policy or needs, alternative models base access control on the discretion of the owner or administrator of the data. Under all alternative models, an end-user's identity determines which access permissions are needed.

This section describes the other three predominant access control models:

- access control lists (ACLs),
- DAC, and
- MAC.

Figure 2-3 compares RBAC to other access control technologies.

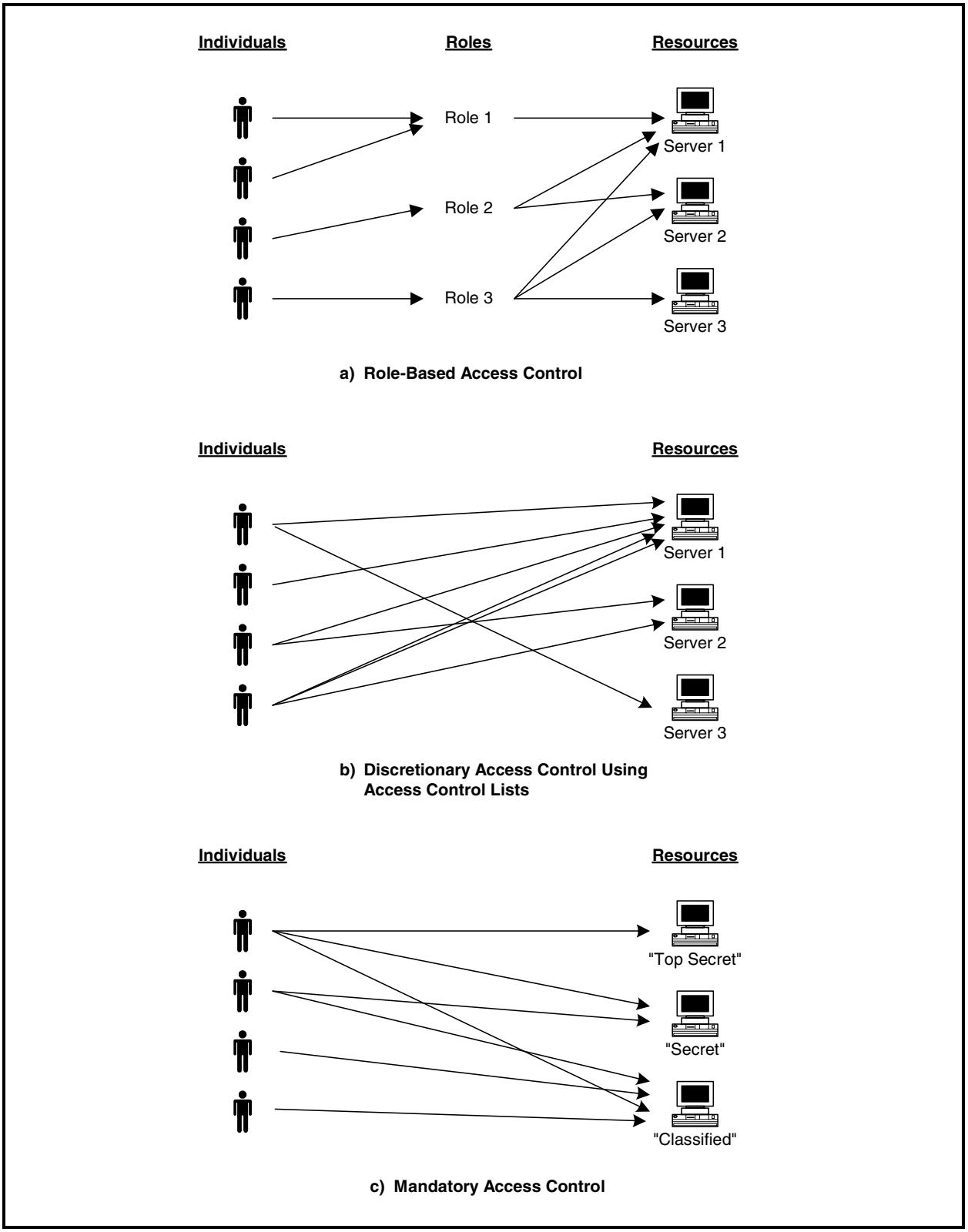
Access Control Lists

One of the most common access control models is the use of ACLs. When using ACLs, every piece of data, database, or application has a list of users associated with it who are allowed access. In this system, it is very easy for the security administrator to see which users have access to which data and applications. Changing access to the piece of information is straightforward; an administrator simply adds or deletes a user from the ACL.

Each set of data or application has its own ACL, but there may or may not be a corresponding list that gives the network administrator information on all of the pieces of information to which a particular user has access. Only by examining each piece of data individually and checking for access can the security administrator find any potential security violations. If all accesses by a particular user need to be revoked, the administrator must examine each ACL, one by one, and remove the user from each list.

When a user takes on different responsibilities within the organization, the problem gets worse. Rather than simply eliminating the user from every ACL, the network administrator must determine which permissions need to be eliminated, left in

Figure 2-3. Alternative Access Control Technologies
RBAC offers a more efficient method for assigning users access permissions than alternative access control models.



place, or altered. Network administrators have made several attempts to improve ACLs. In some cases, users can be put into groups, making it easier to change the ACL. In other cases, elaborate rules can be applied to ACLs to limit access to particular pieces of data.

Discretionary Access Control

The main concept of DAC is that the individual who owns the data is able to control access to the data. ACLs are regarded as one implementation of DAC. DAC governs access to information based on the user's identity and rules that specify which users have access to which pieces of information. Whereas ACLs are lists that specify which users can access a particular piece of data, DAC consists of a set of rules that specify which users are allowed to access the data. When a user requests access to a particular piece of data, the server searches for a rule that specifies which users are allowed to access the information. If the rule is found, the user is given access; if not, the user is denied. For example, a rule may state that users from a certain group are not allowed to read a particular data file.

Rule-based DAC is an improvement over ACLs, but it is still susceptible to human error and therefore suffers from potential security violations. DAC does not impose any restrictions on data access for a particular user. Once users can access data, they can change or pass that information onto any other user without the security administrator's knowledge (Sandhu and Samarati, 1994).

Mandatory Access Control

MAC is a departure from other access control mechanisms because it is based on hierarchical security labels and assigns each user and each piece of information or application a particular security level (e.g., classified, secret, top secret). Two common principles are then applied to determine if a user has access to a particular piece of information: read down access and write up access.

Read down access gives users the ability to access any piece of information that is at or below their own security level. If a user has a secret security level, they are able to access secret and classified material but not top secret material. Write up access states that a subject's clearance must be dominated by the security level of the data or information generated. For example, someone

with a secret clearance can only write things that are secret or top secret. With these two access control principles, information can only flow across security levels or up security levels.

2.2 BENEFITS OF RBAC

Using roles to determine and manage access permissions allows system administrators to better incorporate least privilege and separation of duties into administrative policies. As discussed, RBAC exists in many forms, but even its simplest form is an improvement over alternative methods. "RBAC features such as policy neutrality, principle of least privilege, and ease of management make [RBAC models] especially suitable candidates…Such models can express both DAC and MAC policies, as well as user-specific policies. In essence, RBAC models can provide generic framework for expressing diverse security requirements" (Joshi et al., 2001a).

In this section, we discuss the types of benefits associated with using RBAC rather than another method. Key benefits are

- ➤ simplified systems administration,
- ➤ enhanced organizational productivity,
- ➤ reduction in new employee downtime,
- ➤ enhanced systems security and integrity, and
- ➤ simplified regulatory compliance.

2.2.1 Simplified Systems Administration

Once an RBAC system is established, the costs associated with administering and monitoring the network are less than those associated with alternative access control models. Several factors influence the magnitude of the cost decrease. First, the greater employee turnover, and in turn the number of people changing roles, the greater the cost savings of RBAC relative to other access control systems. Second, some firms or organizations are very dynamic, and user roles and permissions change quickly. In these environments, RBAC is more efficient in moving users in and out of given roles and changing the permissions of given roles than competing access control systems. This improved efficiency is observable in the decrease in labor hours that the computer network support team spends on administrative tasks.

In addition to reducing system administration costs, the automated access control systems supported by RBAC reduce the burden on upper management. In alternative access control systems, upper management is integrally involved in determining individual privileges and authorizing access for each new employee. RBAC's organizational structure supports the automation of this process.[1]

Several issues must be weighed when granting access permissions. Security administrators need to balance the

- complexity of the position being assigned privileges,
- complexity of the organization,
- security level required,
- data and application needs of the position, and
- organizational issues.

By assigning a predetermined role to the user, the labor expense of assigning permissions is significantly reduced, thus freeing labor resources for other tasks.

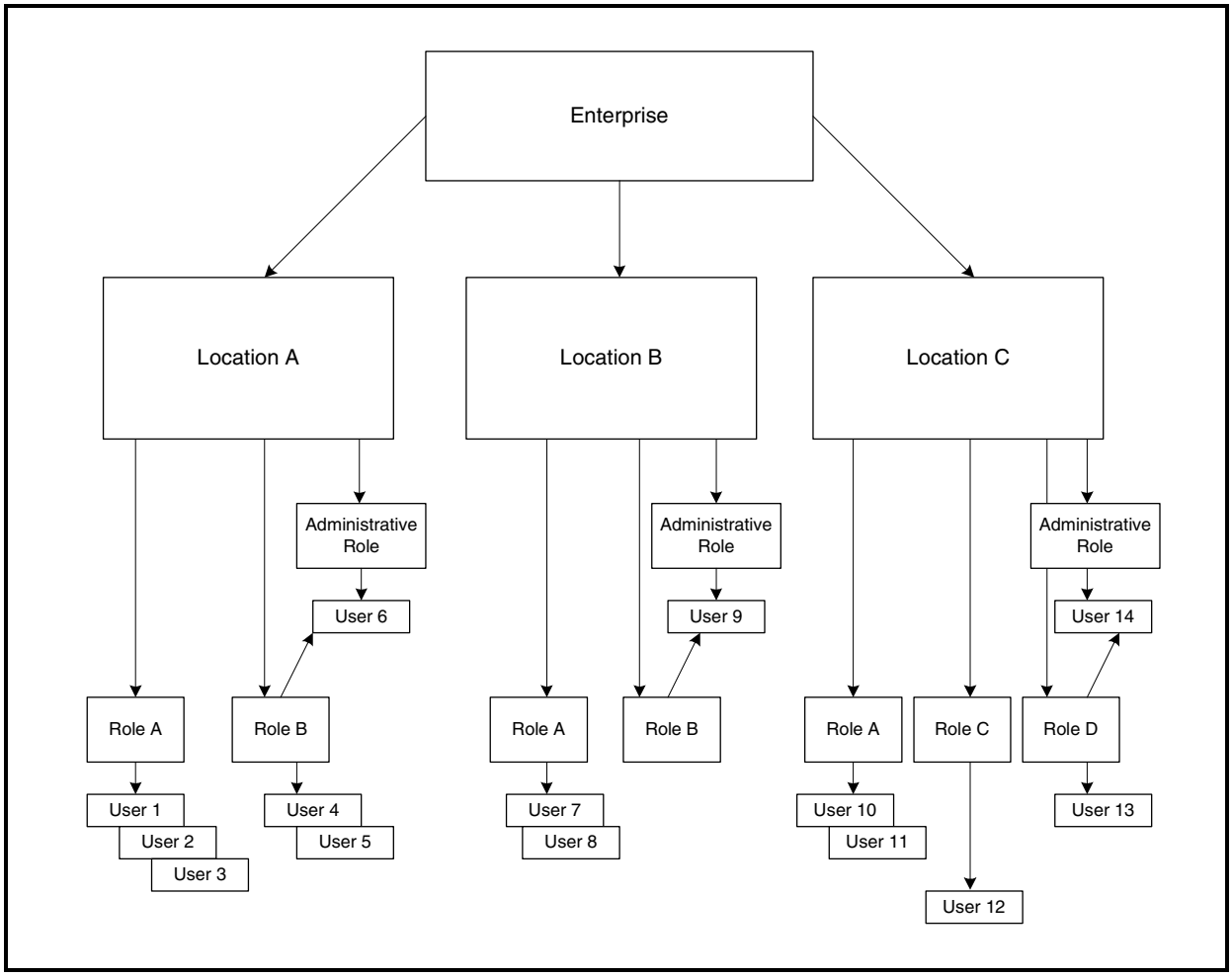
RBAC is a scalable model, meaning that the model can work as well in large environments covering several offices and classes of users as it can in one-office environments. Roles matching job positions may be determined in a central office, but the actual assigning of roles to or changing of roles for new employees can occur at each branch office by an administrator. This concept, frequently referred to as delegated administration, can be of particular benefit to organizations with several branch, subsidiary, or contractor locations, such as health care plans, insurance companies, banks, and similar organizations (see Figure 2-4).

2.2.2 Enhanced Organizational Productivity

RBAC also has the potential to enhance the system by which firms and organizations structure their information systems. Because of the greater flexibility and breadth of network design associated with RBAC, the model can be adapted to mirror the organizational structure. This creates the potential for new and innovative ways of structuring the organization, altering the routing of information, or changing the organization's production processes. Organizations

[1] Industry experts indicated that automation was possible with alternative access control methods; however, the concept of roles greatly enhanced the benefits associated with automation.

Figure 2-4. An Example of Delegation Administration
An enterprise can distribute the burden of maintaining access permissions by creating administrative roles for its constituent organizations and locations, thereby reducing turnaround times and enhancing productivity.



Source: Courtesy of OpenNetwork Technologies, Inc.

can benefit from the consistency in infrastructure across divisions or units within the same entity. Additionally, improved business standards may result in cost savings. The synergistic improvements that may occur within a company could have potentially large impacts on employee productivity.

2.2.3 Reduction in New Employee Downtime

RBAC accelerates bringing new employees to full productivity. New employees are employees that are new to the organization or are existing employees that are placed in a new position within the company. During this time period, new employees may only be marginally or partially productive. RBAC can reduce the time for

establishing access, and the RBAC structure enables the automation of establishing and verifying access.

2.2.4 Enhanced Systems Security and Integrity

Role-based access models offer improved security and audit trails over alternative methods. RBAC is able to reduce the impact from security violations in two ways. First, RBAC can decrease the likelihood that a security violation occurs. Second, if a security violation occurs, RBAC can limit the damage from the violation. Roles limit the possibility of internal security breaches from individuals who should not have access to the data and applications associated with each function. Furthermore, because privileges are not assigned manually, it is less likely that the security administrator will make an error and inadvertently grant a user access to information or applications to which he or she would otherwise be prohibited.

Additionally, productivity may increase from RBAC's improved security of network resources and increased information access. As a result, companies may increase their confidence in their computer systems and be able to increase the sharing of resources, being less concerned about potential security violations.

2.2.5 Simplified Regulatory Compliance

Several risk factors are inherent in the new mode of conducting business. "Contract employees and outsourced business functions expose critical systems and data to staff that have not been screened, or that may be subjected to uncontrolled turnover…current security administration systems cannot handle the increased complexity induced by these environments" (Byrnes, 1997).

In an age of increasing electronic integration, data security and integrity have become political and economic issues. Incidences of breaches in data security are well documented, as is the sharing of personal information among companies trying to find a stronger foothold in today's highly competitive markets.

To protect the confidentiality of both individuals and their personally identifiable information, recent federal laws have included provisions that dictate the type and the extent to which individuals' information can be shared both within an organization and with others. These laws, including the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) of 1999, require data managers to securely maintain and limit the distribution of data. To comply, companies are required to use access control policies that will safeguard data. RBAC is one such policy that may be best suited for this purpose. This section discusses recent Acts and the way RBAC supports compliance.

The Health Insurance Portability and Accountability Act

HIPAA is a health care reform initiative enacted in 1996 to add a dimension of portability to workers' health insurance as they transition between states of employment. HIPAA also contains privacy provisions that apply to health information created or maintained by health care providers who engage in certain electronic transactions, such as health plans, and health care clearinghouses. To meet privacy compliance obligations, entities must maintain secure information systems that have the functionality to prevent the willful or unintentional disclosure of any individual's health records and or personal information to unauthorized parties.

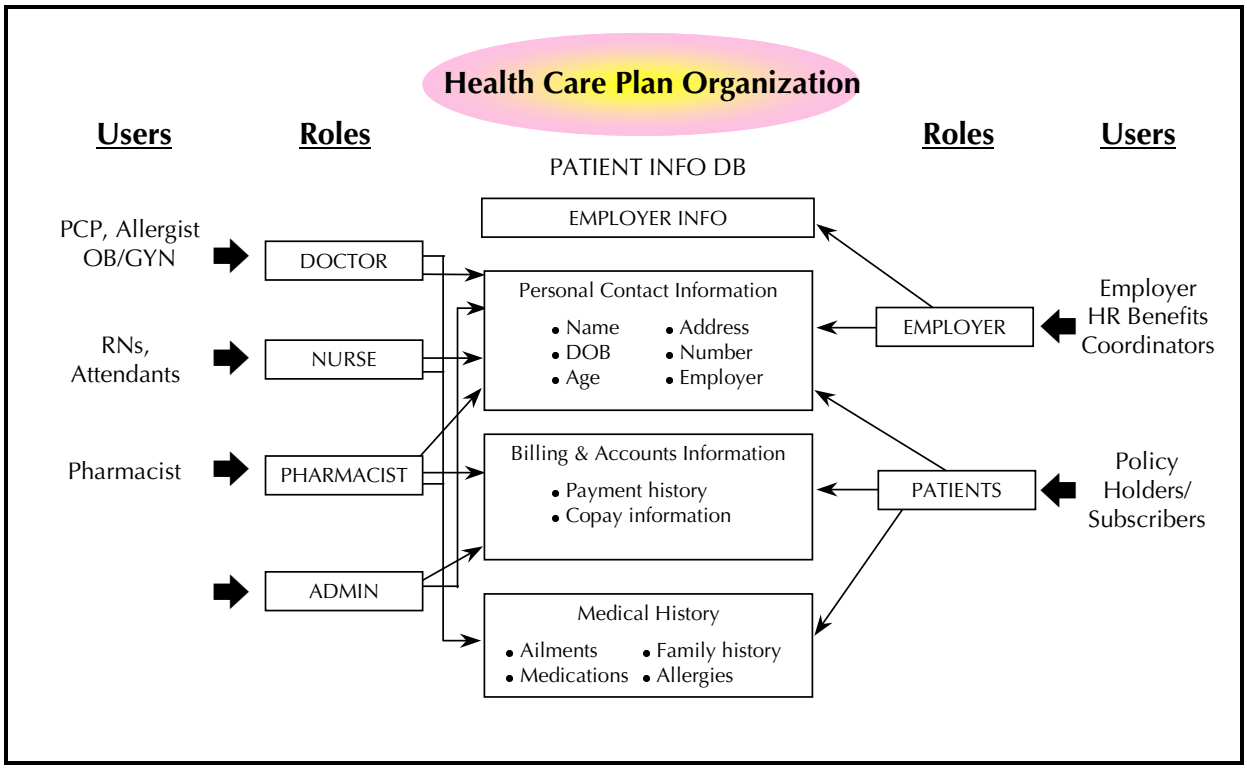
RBAC facilitates HIPAA compliance by providing an access control structure that permits only people in certain roles to access certain types of information, such as patients' medical records. For example, a health care provider may assign a contracting physician a certain role that allows the doctor access to medical records, but office staff in charge of billing and administrative tasks may be assigned another role that permits access to claims information but not medical records.

Although HIPAA does not explicitly mention any given access control model in the final rule, its implementer, the Department of Health and Human Services (DHHS), specifically espouses RBAC as a security model to safeguard health data.

Although HIPAA does not explicitly mention any given access control model in the final rule, its implementer, the Department of Health and Human Services (DHHS), specifically espouses RBAC as a security model to safeguard health data. In fact, DHHS's Health Care Financing Administration (HCFA) refers queries about role-based access to NIST publications and the NIST web site in its "General Questions" section about HIPAA. Responding to one question about role-based access, HCFA writes "please review Chapter 17—'Logical Access Control' of NIST SP 800-12, 'An Introduction to Computer Security: The NIST Handbook'" (HCFA, 2001).

Figure 2-5 is a simplified example of how RBAC can be used to comply with HIPPA from the perspective of the health care organization (HCO). Using an RBAC system, the HCO can limit which users can access which types of data. For example, a billing clerk at a doctor's office may access a patient's contact and billing information but not her medical history. A doctor, on the other hand, has full access to the patient's medical history.

Figure 2-5. Heath Care Industry Example of Using RBAC to Control Access to Sensitive Information
Organizations in the health care industry can leverage RBAC to meet HIPAA requirements by allowing only users in select roles to access particular data.



Other Acts

In addition to HIPAA, several other Acts were enacted in the late 1990s that include extensive provisions concerning the privacy of consumers' personal information. These include the GLBA of 1999 and the Telecommunications Act (Telecom Act) of 1996. The GLBA eliminates the barriers between banking, investment banking, and insurance activities and companies dating from the Depression-era Glass-Steagall Act. Similarly, the Telecom Act, intended to increase and allow competition in telecommunications, allows communications business to enter any market and to compete against each other.

Although the main goal of both the GLBA and the Telecom Act is to increase competition in previously tightly regulated markets, the new provisions for the protection of consumer information generated some of the most interest (Ledig, 2000). Both Acts specify the manner in which personal data can be exchanged

among companies and among divisions of companies. They also lay out which information must be held in confidence and which may be distributed in aggregate form, if at all. The GLBA goes further than the Telecom Act by giving consumers the authority to block the exchange of any information concerning themselves or their accounts among or within companies except as concerns the maintenance of their accounts. Although neither Act indicates or explicitly requires an access control method, RBAC is one way through which companies can restrict which classes of information may be viewed by certain types of users.

2.3 RBAC-ENABLED PRODUCT SUPPLY CHAIN

Several software companies produce RBAC and RBAC-enabled software. These products range from commercially available off-the-shelf to custom-designed software. The majority of commercially available products are designed to manage access permissions to information resources within an enterprise's networked environments, such as local-area or wide-area networks, referred to collectively as the intranet environment. However, a significant growth area in the near future will be for RBAC products managing Internet-accessible systems, also referred to as extranets.

Although Internet-based applications would have existed with or without RBAC, RBAC decreases the administration and maintenance costs of these applications and enhances their security.

Most of the examples in this report approach RBAC from the perspective of its use in the intranet environment. However, neither RBAC's application and technical characteristics nor its benefits or costs differ by environment. There is little difference in the technology or methodology of defining and creating roles and incorporating applications between the intranet and the Internet environments.

RBAC via the Internet supports and enhances business activities by more efficiently connecting end users to Internet-based applications. Although Internet-based applications would have existed with or without RBAC, RBAC decreases the administration and maintenance costs of these applications and enhances their security (Joshi et al., 2001b). To deliver these applications over the Internet, different classes of end users, such as customers or contractors, may be assigned roles to maintain or verify their own accounts, reducing the administrative load on the firm. Once these end users have enrolled, they may be able to register and maintain

account information, alter their product or service packages, submit requests or questions, and settle payments. In such a large computing environment, it may be desirable to have users register and maintain their own accounts.

It should be stated here that RBAC's application is not limited to managing permissions in networked environments. Individual databases or applications may also have an RBAC system. Although the economic benefits of RBAC are hypothesized to be concentrated in RBAC's use in networked environments, RBAC will also be used to manage access to any form of information resource, including data sets, applications, or other systems. An enterprise does not need to have an RBAC policy mapped to its organizational structure in these instances, but a policy that is naturally mapped against that particular resource's user structure. Even in such a focused application, the owner of that resource accrues both the benefits and costs of RBAC.

2.3.1 Software Developers

Software developers design, program, and market systems and applications software to manage user access. These software packages may or may not have the ability to control user access using roles. Those that do are said to be RBAC-enabled or have RBAC functionality. Software that is RBAC-enabled has a module or administrative tool feature that allows an administrator to create and restrict access to roles. Some software vendors offer an optional RBAC module that can be integrated with their customers' software suites. Presently, most software systems with RBAC functionality are systems software.

At the time this study was completed, relatively few software developers had RBAC-enabled products commercially available. However, software developers forecast that the market for such products will increase significantly, driven by information security and privacy concerns. Table 2-1 lists some firms that currently market RBAC and RBAC-enabled software. These firms' software products fall into several categories, including security management, electronic commerce infrastructure and platforms, operating systems, and access control, with most products belonging to more than one category.

Table 2-1. Sampling of Software Developers Currently Offering RBAC and RBAC-Enabled Products

Several software developers currently offer RBAC and RBAC-enabled products. The list below is representative of firms that offer package solutions. It should be noted that other types of firms not listed here, including computer consulting firms, may offer custom-designed solutions. Some end users also design RBAC systems in-house.

Access360, Inc.	RSA Security, Inc.
Adexa, Inc.	Secure Computing Corp.
BEA Systems, Inc.	Siemens AG
Cisco Systems, Inc.	SETA Corp.
Entrust, Inc.	Sun Microsytems, Inc.
Entrust Information Security Corp.	Sybase, Inc.
International Business Machines Corp.	Symantec Corp.
Internet Security Systems, Inc.	Systor AG
iPlanet E-Commerce Solutions	Tivoli Systems, Inc.
Microsoft Corp.	Vignette Corp.
Network Associates, Inc.	Baltimore Technologies, Inc.
OpenNetwork Technologies, Inc.	BMC Software, Inc.
Oracle Corp.	Novell Corp.
PGP Security, Inc	Radiant Logic, Inc.
Protegrity, Inc.	

2.3.2 End Users

RBAC can be used in almost any sector that uses a computer network to limit user access to particular pieces of information. But RBAC is most likely to be of significant benefit to organizations with many employees and/or multiple locations. The following sectors are likely to have the highest RBAC adoption rates:

- banking,
- health care,
- government agencies,
- telecommunications,

- computer applications security, and
- military.

A recent report by SETA Corporation (1996) for NIST points out that certain characteristics within specific firms or sectors magnify the benefits from RBAC. These characteristics include, but are not limited to,

- User Characteristics
  - ✓ a large number of users
  - ✓ few security administrators
  - ✓ high turnover rate
  - ✓ large number of data objects
- Data Characteristics
  - ✓ stable set of applications
  - ✓ little change of roles within firm
  - ✓ job-dependent access to information
  - ✓ stable organizational structure
- Organizational Characteristics
  - ✓ the organization owns the data and applications
  - ✓ the organization controls data and application access
  - ✓ user accountability is required within the organization
  - ✓ reassessment of the access control policy occurs within the organization

3 Barriers to RBAC Development and Implementation and NIST's Contributions

Two general categories of market failures affect RBAC: barriers to the technological development and integration of RBAC into software products, and barriers to adoption and implementation of RBAC-enabled products by end users. We address the first set of barriers, which primarily affect software developers (and in-house developers) of RBAC-enabled products and are in large part due to RBAC's generic technology attributes. We discuss RBAC's infratechnology-related market barriers that primarily affect adoption and implementation by end users. The section concludes with an overview of NIST's response to these market failures through its RBAC project.

3.1 BARRIERS TO TECHNOLOGY DEVELOPMENT AND INTEGRATION OF RBAC MODELS INTO SOFTWARE PRODUCTS

The barriers to private-sector development and integration of RBAC into software products stem from the uncertainty about the success and costs of the applied research and product development and the difficulties in appropriating returns to their R&D investments. These barriers are rooted in the concept of generic technologies, which have many of the characteristics of public goods. Generic implies that once a base model has been developed it may be easily applied in numerous other commercial settings, including

other companies appropriating the model for use in competing products.[1] RBAC is a generic technology for this very reason. The development of generic technologies is generally slow because they can be applied in numerous settings, industries, or firms. Additionally, because once the knowledge is generated and the standardization of a technique occurs, appropriating the benefits to the innovating entity is difficult.

"The market will fail to provide sufficient infrastructure because of appropriability and risk problems. These are, of course, the essential problems that cause markets to fail more generally in R&D activities, resulting in underinvestment from society's perspective" (Scott, 1999).

Generic technologies are similar to public goods in that they have the characteristics of nonrivalry and nonexcludability.[2] RBAC is nonrival because one firm's use of RBAC does not affect another firm's use. RBAC is also nonexcludable because one firm cannot prevent another firm from using the fundamental concepts of roles as the basic technology is advanced. Public goods are typically underprovided by private markets as compared to their socially optimal levels of provision (Stiglitz, 1988).

This section discusses the barriers to developing and integrating RBAC models in commercial software products that result from RBAC's generic technology characteristics. These barriers include the

- need for technical expertise outside the software industry's domain,
- lack of a consistent definition for RBAC, and
- difficulty in appropriating returns to investment.

The first two factors lead to uncertainty in the success and costs of RBAC R&D. The third factor leads to uncertainty in the company's ability to appropriate returns from its RBAC investments. All of these factors can delay the availability of RBAC-enabled products. When appropriate, we discuss NIST's role in addressing these

[1] Although RBAC is an important concept for developing access control systems, it should not be considered an infratechnology. Infratechnologies are technical tools, including scientific and engineering data, measurement and test methods, and practices and techniques, that are widely used in industry (Tassey, 1997). RBAC is not an infratechnology because its main effect is to provide a technology platform (i.e., a generic technology) rather than leverage the efficiency of R&D, production, or market transactions.

[2] Public goods, unlike private goods, are characterized by consumption nonrivalry and by high costs of exclusion. Rationing of such goods is undesirable because the consumption of a public good does not impose costs on society because it does not reduce the amount of the good available to others. Further, the costs of excluding those who do not pay for the infratechnologies are likely to be high because they are typically embodied in products and processes (techniques), rather than in products that can be sold.

market failures. A more detailed discussion of NIST's specific activities and expenditures is included in Section 3.3.

3.1.1 Technical Expertise Outside the Software Industry's Domain

Although the fundamental concepts of roles are common knowledge, the capability to formalize model specifications needed to implement RBAC models is beyond the knowledge base of existing staff in many software companies. The lack of understanding of the programming requirements or a lack of awareness of RBAC models makes software companies hesitant to commit to RBAC development.

The lack of knowledge and staff expertise in the area of RBAC increases the uncertainty of both the technical feasibility of developing successful RBAC-enabled products and the development costs and time frame. These uncertainties increase the project risk and create significant barriers to investment in new RBAC-enabled software products. The risk impacts are further magnified by the fact that most business managers (decision makers) are risk adverse, weighing potential downsides greater than equivalent potential upsides in the probability distribution of returns.

NIST's RBAC project addresses these market failures by demonstrating the technical feasibility of RBAC products through its programs. In addition, NIST's patents, papers, and the conferences it has sponsored disseminate the basic RBAC generic technology from which private companies can develop market applications.

3.1.2 Lack of Consistent Definition

RBAC is a broad open-ended technology that ranges from very simple role structures to complicated hierarchies and constraints. As a result, the development of a single model is not appropriate. However, the lack of agreement on a set of fundamental concepts and underlying terminologies created a barrier to the development of RBAC-enabled products in the 1990s.

As with the development of many new technologies, evolving RBAC models have typically used different terminology to describe similar concepts and functionalities. The fact that RBAC has

simultaneously emerged from many different commercial and academic backgrounds has also contributed to the lack of consistent definitions and has increased confusion.

The lack of consistent definitions has slowed the implementation of RBAC. As a result, software develops have difficulty leveraging publicly available information and consumers of RBAC products have difficulty evaluating and comparing different products. The development of the NIST model was one of the first attempts at presenting industry with a set of consensus RBAC concepts and terminology. NIST has followed this model development with a proposed standard for RBAC, which was developed in collaboration with industry and academics.

3.1.3 Difficulty of Appropriating Returns to Investment

RBAC models are generic technologies that can benefit a wide range of industries. It is a technology that will be integrated into a variety of products targeted at different market segments. As a result, it is difficult for the individual companies in the private sector to fully appropriate the returns from their investments in RBAC because technology spillovers and imitation are likely to be high. For firms to engage in R&D to develop a new technology, several conditions need to be in place. One of these is the ability to appropriate the market returns that are generated when a new technology is introduced into the marketplace. Market returns to R&D can take two separate forms: private and social. Private returns can be thought of as the profits that individual firms receive from selling the new technology—the price per good minus the R&D and production costs. Social returns are the benefits that accrue to all of the other participants in the market in which the technology was implemented or other markets that may benefit from using that technology. Jaffe (1996) describes these benefits as "spillovers." For example, when a firm engages in R&D, other firms learn what has worked and what has not worked. They can than reverse-engineer the process or otherwise gain "knowledge" from the activities of the first firm. Because firms cannot fully appropriate the spillovers, firms underinvest relative to the socially optimal rate.

However, the existence of market spillovers does not constitute a need for government action; other conditions must also be met. If

the private return is large, there may be enough of a market incentive for the innovating firm to still engage in R&D. Additionally, the innovating firm may be be able to capture enough of a private return that they would still invest in the technology. Jaffe points out that knowledge spillovers are a market failure when private returns fail to reach a specific societal hurdle rate when the social returns do. In these cases, suboptimal investment is likely to occur.

One way for a company to appropriate the returns from R&D is to limit the spread or use of its technical innovations through secrecy, patents, or licenses. However, in the case of RBAC, because it is embodied as a software product, it is difficult to prevent imitation through reverse engineering. Similar, patents and licenses provide less protection for software products compared to other areas of technology innovation because competing firms are frequently able to "invent around" the existing patent, effectively preventing the innovating firm from appropriating all of the returns associated with an innovation.

Because of the appropriablity issues discussed above, it is generally accepted that government needs to fund research in generic technologies to the point where market applications become profitable for the private sector (i.e., where the risk-adjusted expected rate of return to investment in RBAC products exceeds the companies' internal rate of return criteria) (Scott, 1999). NIST's involvement mitigates market appropriation issues by providing the research foundation to which all have access. Firms are then able to produce and market products that build on NIST's research and therefore incur only the incremental R&D costs for orienting the RBAC applications needs of their current and prospective products towards their customer base. This makes investment in RBAC-enabled products more attractive for the private sector and accelerates the availability of commercial RBAC-enabled products.

A second advantage of this approach by NIST is the limitation of users being locked into a specific product or firm. When the generic technology is publicly available, software products from competing companies are more likely to be interoperable and work together in integrated systems. This increases competition and lowers barriers to entry in the access control market.

3.2 BARRIERS TO IMPLEMENTATION OF RBAC-ENABLED PRODUCTS

The second category of barriers to developing and adopting RBAC is implementation barriers that affect end-user investment decisions. These barriers can affect an end-user organization's decision of whether to implement a role-based access policy and hence RBAC-enabled products. Many of the tools needed to support end users' adoption of RBAC fall into the category of infratechnologies.

Software end users who responded to our Internet survey concurred on the factors that are important in choosing an access control technology. These factors are

- ease of installation and management,
- level of security provided,
- ability to cover most platforms,
- scalability,
- ease of use,
- costs of implementation, and
- complexity of implementation and maintenance.

In an ideal scenario, an organization will establish and design operations processes and then create an infrastructure that will execute those processes, providing to each member only the tools needed to perform one's function (Byrnes, 1997). Information systems are designed and built to support the roles that correspond to these processes. Each role is assigned a series of permissions defined by their position and function within the organization. Ideally, the system is clearly defined and agile, making the addition of new applications, roles, and employees as efficient as possible.

According to software developers and end users, however, the ideal scenario rarely occurs. Business processes and employee positions, both formal and informal, are preexisting and entrenched, impeding turn-key implementation of new systems and management philosophies. Because RBAC requires roles to be established within the workplace, organizations implementing a role-based system may need to complement their information access policies with their general administration policies. Subsequent realigning of workflow and positions, to whatever extent necessary, may be very expensive, difficult, and time consuming.

One software developer noted that

> RBAC [is] a tool that supports a correctly defined [administrative] policy….The structure and support model of the organization, as defined by that policy, will determine the cost savings, if any, should RBAC be implemented. Actually, RBAC will cost an organization more in the long run if the policy for that organization is not realistic in terms of operational requirements for RBAC or fails to even define RBAC and its use throughout the organization.

This section discusses the impediments for current and potential end users beyond the direct cost of purchasing the software of installing RBAC. These impediments are not insurmountable, but they do factor into organizations' business decisions concerning adoption. Herein we depart from analyzing RBAC as a software component and take the position of a potential end user, focusing on the issues that arise during RBAC adoption. Interviews with software developers, end users, and technical specialists as well as articles in the popular press inform our discussion of implementation impediments. These impediments are divided into three general categories: role engineering, migration costs, and systems structure.

3.2.1 Role Engineering

One developer said a customer's rollout of RBAC hit a large number of glitches precisely because "the overriding problem can be traced back to a lack of RBAC support in the organization's administration policy."

The process of defining and implementing roles is known as "role definition" or "role engineering." According to the software developers interviewed, role engineering can be a contentious and time-consuming process, but it is integral to RBAC's success. One developer said a customer's rollout of RBAC hit a large number of glitches precisely because "the overriding problem can be traced back to a lack of RBAC support in the organization's administration policy."

Role engineering entails defining the roles that will determine which employees have access to which data and to which applications. Also determined are roles' relationships to one another, role hierarchy, and role constraints. As this process progresses, implementers may see benefits in rethinking how work is allocated and completed within the organization. Role engineering may be the costliest component of implementation because, even for an $RBAC_0$ system, defining roles may take 3 to 4 months according to developers.

Workflow processes may be realigned as informal access grants are formalized and roles defined. Transitioning to a role-based system formalizes many relationships within an organization (Byrnes, 1997). This process may have the added benefit of introducing organizational clarity into the workplace. Many organizations grant ad-hoc access control as new applications are installed or job definitions change. The changeover to a centralized system may bring many of those types of issues to bear.

It is expected that role-engineering expense will decrease over time because of the development of new software tools and increased familiarity with the process of defining and assigning roles. Several companies have developed or are in the process of developing software tools that help to automatically define roles using existing patterns of access permissions gleaned from user databases. These tools should reduce the labor expense of manually defining and creating all roles. Furthermore, as companies and consultants become familiar with the implementation process, a learning curve effect should emerge. What is not clear, however, is what the total impact on role engineering these two developments will have. The relative ease or difficulty of the role definition process will depend on an entity's organizational and administrative structure, an attribute that varies widely among firms.

NIST has developed specific tools to assist end users in role engineering. The tools include RGP-Admin, a tool for managing role/permission relationships, and AccesMgr, a graphical user interface for managing access control lists for Windows NT files. Through the development of these tools NIST has lowered the cost, and hence the barrier, to adopting and implementing RBAC-enabled systems.

3.2.2 Migration Costs

Any time a new information system is installed, an organization will accrue costs. This is especially true if the decision is to implement a new access control system. The costs of migrating to a role-based system are four fold: salaries and consultants' fees, software purchases and licensing agreements, computing resources and infrastructure, and customization costs. These costs may differ depending on the scope of the package being installed, the size of the firm or the number of licenses, and the migration complexity.

One of the largest cost components of installing an RBAC system is the salaries and benefits of the team tasked with its implementation. Tasks include not only the implementation and migration of the software system purchased, but also the staff training, software package selection, and the customization process. In addition to staff labor expenses, consultants may be hired to either implement the systems migration completely or to offer their expertise on some

component therein. Outside consultants may also be hired to customize a prepackaged system or help with role definition.

In addition to purchasing the software itself, an organization may invest in software support services and new systems infrastructure. The software agreement may involve a sliding fee scale based on the number of licenses purchased and a software maintenance agreement. Depending on the package's system requirements, buyers may need to build or enhance their systems' infrastructure. The expense of buying, installing, and maintaining computing resources can be high. Costs may rise further if network resources must be maintained solely or partly to help migrate from one system to another.

Although NIST has not specifically focused its efforts on how firms can migrate from one access control system to RBAC, the migration and transaction costs from migration to RBAC have slowed its adoption. Future work by NIST in supporting migration from other access control systems to RBAC may be valuable.

3.2.3 Systems Structure and Interoperability

If a large firm with access control concerns could choose today an access control system to use, most would choose RBAC. However, most firms made the decision on how to control access to information before RBAC was a candidate. The choice set included ACLs, DAC, and MAC. Once the access control system decision was made and implemented, networks evolved through time and became firm specific. User definitions and permissions were created based on the potentially thousands of employees that work for a particular firm. Lock-in of the access control system has occurred in many firms (Hilchenbach, 1997). The market failure associated with this inability to break-out of this problem as slowed the adoption of RBAC by users.

As new systems are installed, administrators may have to rectify years of inefficiencies, such as informal access grants, disorganized systems, and different organization structures among divisions. The move towards disciplined centralized systems often means realigning these systems and creating a more cohesive, formal systems structure.

Because of the time and cost involved, it is likely that a large organization will adopt RBAC at an incremental pace. By spreading out implementation over a period of time or only when new applications or systems come online, companies avoid the risk-prone full rollout.

An additional barrier to developing commercial RBAC products is the wide range of operating systems that users employ. Even within one firm or organization, multiple operating systems are often needed. As firm size increases, so does the number of operating systems (Ferraiolo, Gilbert, and Lynch, 1992). As firm size increases, the importance of access control also grows (*Infosecurity Magazine*, 1999). Because they combine these effects, larger firms need an access control system that is able to operate across multiple operating systems. In addition, security features need to be effective across sectors of the firm or organization without being overly intrusive to the user. This trait is referred to as interoperability. Interoperability is the ability to communicate and transfer data or information across different activities and platforms. For example, an access control system that displays perfect interoperability would be able to communicate with the security and administrative network across an entire firm without any disruptions or complications.

Without a framework or architecture for addressing interoperability problem, firms may be unable to implement RBAC and benefit from the reduced administrative costs and improved security. NIST's activities have been influential in remedying these market failures. Hilchenbach (1997) agrees, "NIST is a driving force behind the move to standardize RBAC." By developing common standards, firms in different industries are now able to implement RBAC across the multiple platforms within their organization, and lessen the lock-in effect. In addition, the development of common standards lays the groundwork for future network externalities across companies. Once a common playing field is established, software developers and network administrators are able to engage in activities that will offer future improvements to RBAC.

3.2.4 Product Acceptance and Comparison

When making purchasing decisions, buyers of software products gather information about the various potential products and then

make a decision based on the comparison of characteristics across products. These comparisons could include cost, quality, reliability, and capacity. For this process to be effective, consumers must have an understanding of what they are getting from a product and producers must be able to prove that they are delivering what the consumer wants.

Without a set of metrics that consumers are willing to accept as standards for a particular piece of technology, software firms are unable to prove that their product is reliable in addressing security issues and effective at reducing administrative costs.

Prior to NIST's involvement, no commonly agreed upon definition of RBAC existed. Without a definition, firms that were interested in either upgrading their existing access control system or purchasing new access control systems may have been unable to compare attributes across commercial RBAC products.

Without a set of metrics that consumers are willing to accept as standards for a particular piece of technology, software firms are unable to prove that their product is reliable in addressing security issues and effective at reducing administrative costs. The entire industry was lacking a yardstick or common definition. If producers and consumers cannot agree on the product they are selling, market transactions are unlikely to happen. A study by NIST (Ferraiolo, Gilbert, and Lynch, 1992) found that part of the reason why RBAC had not been implemented was the lack of a "stamp of approval" from a third party. Ferraiolo, Cugini, and Kuhn (1995) make this clear by stating "The lack of definition makes it difficult for consumers to compare products and for vendors to get credit for the effectiveness of their products in addressing known security problems."

NIST's work at defining RBAC has addressed this failure by engaging in efforts that generate a common yardstick that all software developers can use. Specific projects have included surveys of security needs and the development of a formal RBAC model to demonstrate its effectiveness and reliability. Developing a formal RBAC model is a strategy that has proven successful in other markets.

3.3 NIST RBAC PROJECT ACTIVITIES

Because RBAC has the characteristics of a generic technology, the private sector has been slow to develop it. NIST has responded to the market failures discussed above through a portfolio of activities promoting RBAC's development and adoption. These activities are

targeted at providing the generic technologies and infratechnologies needed by RBAC software developers and end users. NIST's activities have focused on assisting federal agencies in enhancing their access control systems and supporting industry in its development and implementation of RBAC.

NIST/ITL's RBAC project responded to a demonstrated need for improved security mechanisms and standards for administering complex networked systems. At that time, industry believed that a lack of standards was hampering the development of access control products and that a key to the success of such a system would be its ability to operate across a wide range of operating systems (Ferraiolo, Gilbert, and Lynch, 1992).

NIST began work on developing RBAC concepts in 1991. NIST developed a technical report recommending the investigation and use of RBAC within the U.S. Federal Criteria. This study documented the need for federal agency computer networks to evolve from DAC and MAC to address new security and access issues. NIST's RBAC work is being conducted via NIST's Computer Security Division and Software Diagnostics and Performance Testing.

NIST published the first complete RBAC model in October 1992. This early work reflected the integration of several ongoing projects that indirectly contributed to developing the RBAC model. Beginning in 1994, NIST began to fund studies specifically targeted to demonstrate the viability of NIST's RBAC concepts, its commercial potential, and its application to real-world problems.

NIST's major activities in support of RBAC include

- ➤ producing professional publications,
- ➤ applying for patents,
- ➤ sponsoring conferences and workshops, and
- ➤ establishing and funding development and demonstration projects.

NIST has also contributed to the development of infratechnology tools that demonstrate RBAC's potential to end users and support implementation. These tools lower the risk and cost of adoption and provide a springboard to launch the new and emerging market for RBAC-enabled products.

3.3.1 Producing Professional Publications

Table 1-1 lists many of the professional publications NIST staff have authored and co-authored. These publications reflect NIST's pivotal role in the early development stages of RBAC. NIST developed the technical specifications and formal description of the RBAC model (Ferraiolo and Kuhn, 1992). NIST has since expanded the model by incorporating different types of role relationships

(Kuhn, 1997; Gravila and Barkley, 1998; Barkley and Cincotta, 1998).

NIST's publications were an important mechanism for disseminating their research findings to the academic and business communities. NIST's research and subsequent publications provided the technology base from which market applications could be developed. By leveraging NIST's basic research, software developers were able to lower their development costs and accelerate the introduction of RBAC-enabled products.

3.3.2 Applying for Patents

NIST has applied for four patents. They are in the areas of

- implementation of role-based access control in multilevel secure systems,
- workflow management employing role-based access control,
- a method for visualizing and managing role-based policies on identity-based systems, and
- implementation of role/group permission association using object access type.

The purpose of NIST's patents is not to appropriate returns through commercialization of licensing agreements but to ensure that its research would remain in the public domain and be available for all developers of RBAC-enabled products. In this way no individual company or small group of companies can dominate the market and charge monopoly prices that would slow the penetration of RBAC and the realization of its benefits to society.

3.3.3 Sponsoring Conferences and Workshops

NIST has sponsored a number of professional conferences, including a series of ACM workshops on RBAC. In addition to the workshops and demonstrations, the conferences NIST has sponsored have led to the publication of over 100 papers on RBAC concepts and implementation procedures.

These conferences are an important avenue for disseminating information on RBAC development. Timely information dissemination reduces duplicative research efforts and lowers the uncertainty associated with developing and adopting RBAC-enabled products.

3.3.4 Establishing and Funding Development and Demonstration Projects

In addition to NIST's ongoing research to develop generic RBAC technologies, NIST has established and funded studies specifically targeted at demonstrating the viability of RBAC concepts and developing infratechnology tools to support its implementation. Table 3-1 provides an overview of the four main RBAC projects sponsored by NIST.

The tools NIST has developed to assist in implementing RBAC through these projects include RGP-Admin, a tool for managing role/permission relationships, and AccesMgr, a graphical user interface for managing access control lists for Windows NT files. Other examples include the development of specific tools for implementing RBAC for the World Wide Web (Barkley et al., 1997).

In addition, NIST has demonstrated the use of RBAC for the web, for corporate intranets (Ferraiolo, Barkley, and Kuhn, 1999), and for the health care industry (Barkley, 1995). NIST has also assisted with implementing RBAC on the National Security Agency (NSA) Synergy secure operating system.

Through the demonstration of RBAC and the development of tools to support its implementation, NIST has accelerated its market penetration and lowered the cost of implementation of RBAC-enabled products.

3.4 THE IMPACT OF NIST'S CONTRIBUTIONS

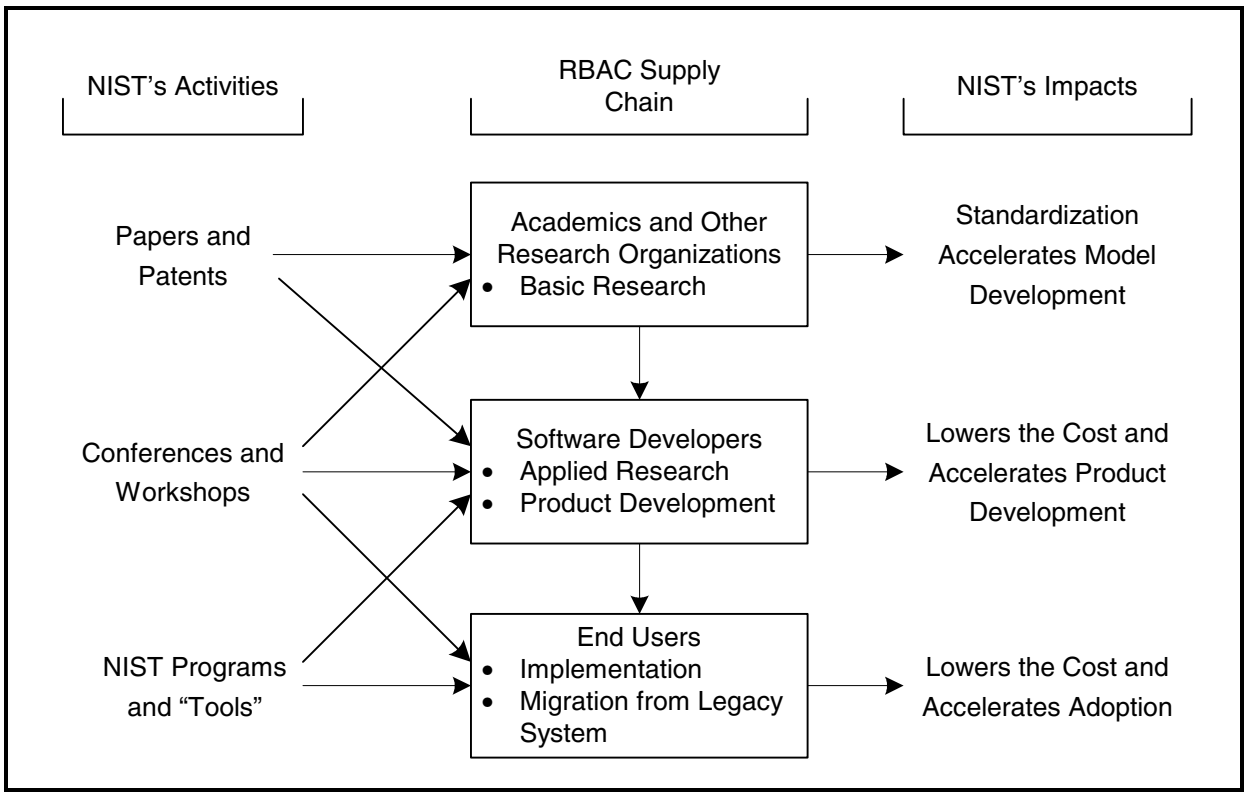
Figure 3-1 shows the impact of NIST/ITL's RBAC project on the access control model development chain and the pathways to benefits attributable to NIST's activities. NIST's role in developing RBAC has primarily been through supporting software designers and implementation companies in developing commercial RBAC software products. However, NIST has also been active within the academic community and in interactions with end users.

NIST's papers and patents have helped to standardize RBAC's terminology and model specifications, which has accelerated RBAC's development as a generic technology. NIST's workshops have helped disseminate information on RBAC to academics,

Table 3-1. NIST-Sponsored RBAC Projects

RBAC for Synergy	
Project Objective	To demonstrate the viability of RBAC concepts and its application to real world problems, the first RBAC prototype was developed on the Synergy platform. This work was performed through using external research funds.
Period of Performance	Developed during the period of October 1994 to December 1996
NIST Project Expenditures	Purchased hardware and software: $50,000 System design and specification, software development and demonstration, and publications: $750,000
RBAC Small Business Innovation Research (SBIR)	
Project Objective	To promote innovative thinking and investigate the commercial implications of RBAC technology, an SBIR topic was developed, selected for funding, and awarded to SETA Corporation.
Period of Performance	September 1994 to June 1997
NIST Project Expenditures	Develop RBAC model and experimentation software: $250,000
RBAC/Web	
Project Objective	To develop an RBAC reference implementation of NIST's RBAC model and demonstrate that the RBAC model applies to networking environment RBAC for the WWW. (RBAC/Web) project was established and was funded using NIST funding.
Period of Performance	January 1997 to December 1998
NIST Project Expenditures	Purchased hardware and software: $40,000 RBAC/Web design and implementation, documentation, APIs, and publications: $574,000
Role Control Center (RCC)	
Project Objective	The RCC was implemented based on a provisional patent application that was filed in August 1998. The purpose of the project is to implement RCC as a Windows NT and Windows 2000 application.
Period of Performance	January 1998 to present
NIST Project Expenditures	$150,000

Figure 3-1. Overview of NIST's Impact
NIST's activities have affected all levels of the RBAC supply chain.



software developers, and potential end users. By promoting the exchange of information these workshops lowered development costs and accelerated the development and adoption of RBAC-enabled products. Finally, NIST projects demonstrated the feasibility of RBAC and provided infratechnology tools to software developers and end users. The demonstrations and resulting tools lowered the cost and accelerated the development and adoption of RBAC-enabled products.

Section 4 presents a conceptual framework from which the impacts of NIST's activities are formally modeled. The model provides the basis for the technical and economic impact metrics that are used to collect information and calculate measures of economic return to the NIST/RBAC project.

4 Analysis Framework

This section presents the modeling approach used to estimate the economic impact of NIST/ITL's RBAC project through its contribution to the development and adoption of RBAC and RBAC-enabled products and services. The approach provides a framework for developing a time series of benefit and costs and guides the data collection activities.

To estimate the economic impacts of NIST/ITL's RBAC project, we needed to develop a time series of benefit and costs for the three key segments of the RBAC supply chain. The time series captures

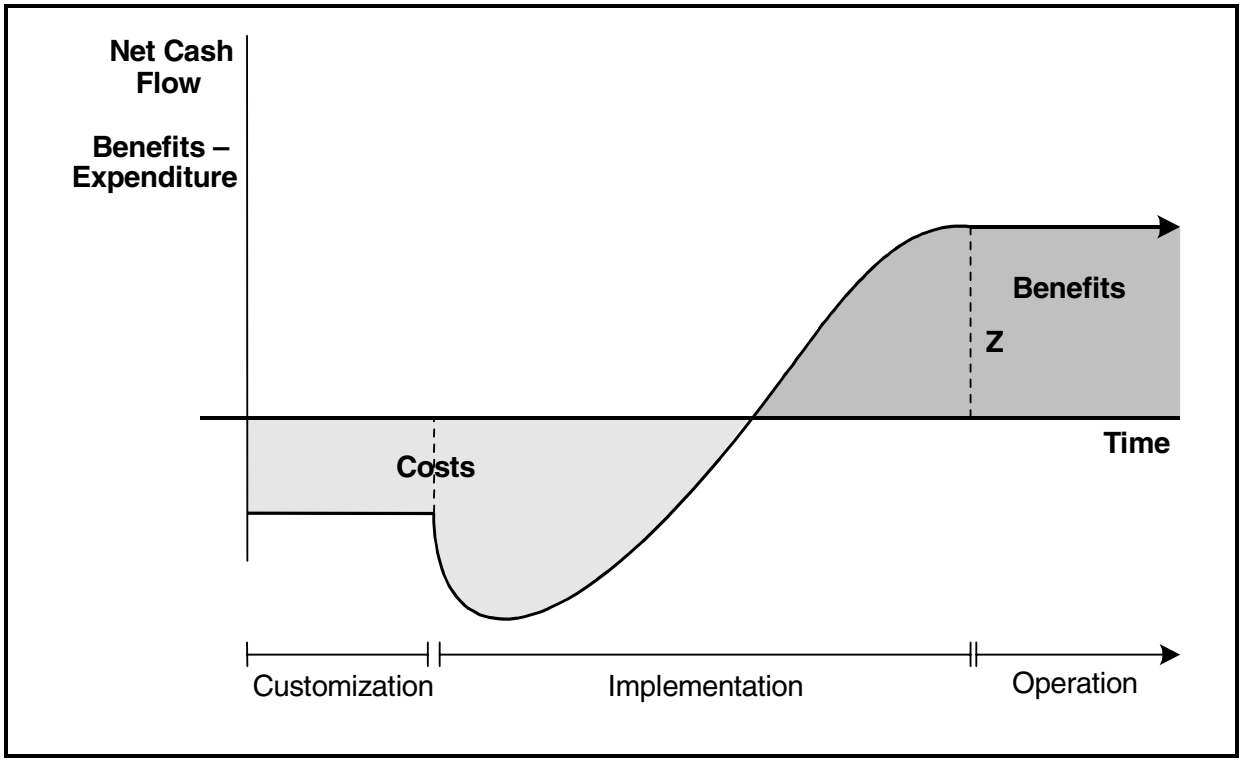
- NIST's expenditures,
- software developers' R&D expenditures with and without NIST, and
- industry users' benefits and adoption costs with and without NIST.

The expenditure time series for NIST and software developers was straightforward to develop and represents a relatively small share of the impacts compared to the industry users' benefit and adoption costs. To estimate RBAC's impact on industry users (with and without NIST), we modeled the representative firm-level benefits of RBAC and its adoption rate by industry. In this section we summarize the impact hypothesis and cost metrics. The section concludes with an overview of the conceptual approach for calculating the measures of economic return to NIST/ITL's RBAC project.

4.1 MODELING FIRM-LEVEL BENEFITS OF COMMERCIAL RBAC PRODUCTS

To estimate the impact of NIST's contributions to the development and adoption of RBAC and RBAC-enabled products and services, we first need to model the flow of benefits and costs associated with RBAC systems. Figure 4-1 illustrates the flow of costs and benefits from the perspective of an individual company associated with installing an RBAC system. These costs and benefits are measured relative to the counterfactual of an alternative access control system such as an ACL, DAC, or MAC that is already in place. Traditional investment theory states that if the net present value (NPV) of the flow of benefits is greater than zero, then the company will undertake the investment project subject to a budget constraint.

Figure 4-1. Flow of End-User Costs and Benefits



As shown in Figure 4-1, the life-cycle of an RBAC system for users can generally be segmented into three phases:

- system customization,
- system implementation, and
- system operations.

System customization includes determining which system is best for the individual firm, purchasing the system, planning the migration, and defining preliminary roles. During this phase an organization produces a comprehensive business plan and prepares to roll out RBAC in its organization. This phase of the project can involve 6 months of planning, on average, during which several tasks must be accomplished. These tasks include customizing software; performing additional programming; developing request and approval processes for changes in user assignments; and developing a set of roles, role hierarchies, and role restriction/interactions that clearly capture the company's business activities. The organization determines what roles need to be created and what information needs to be associated with which role. Although role definition begins during this phase, it is an iterative process, and roles will evolve and be redefined over time. System implementation is a two-phase process that involves rolling out the new systems to end users and reestablishing user privileges via roles. First, information administrators must determine the privileges that each user needs based on her job function. Second, they must determine and define the role that corresponds to their particular job function. Implementation can be the most costly part of the project and typically occurs over 6 months. Some benefits of RBAC will be realized soon after implementation begins, as employees are gradually converted to the RBAC system and as new employees are processed using the new system.

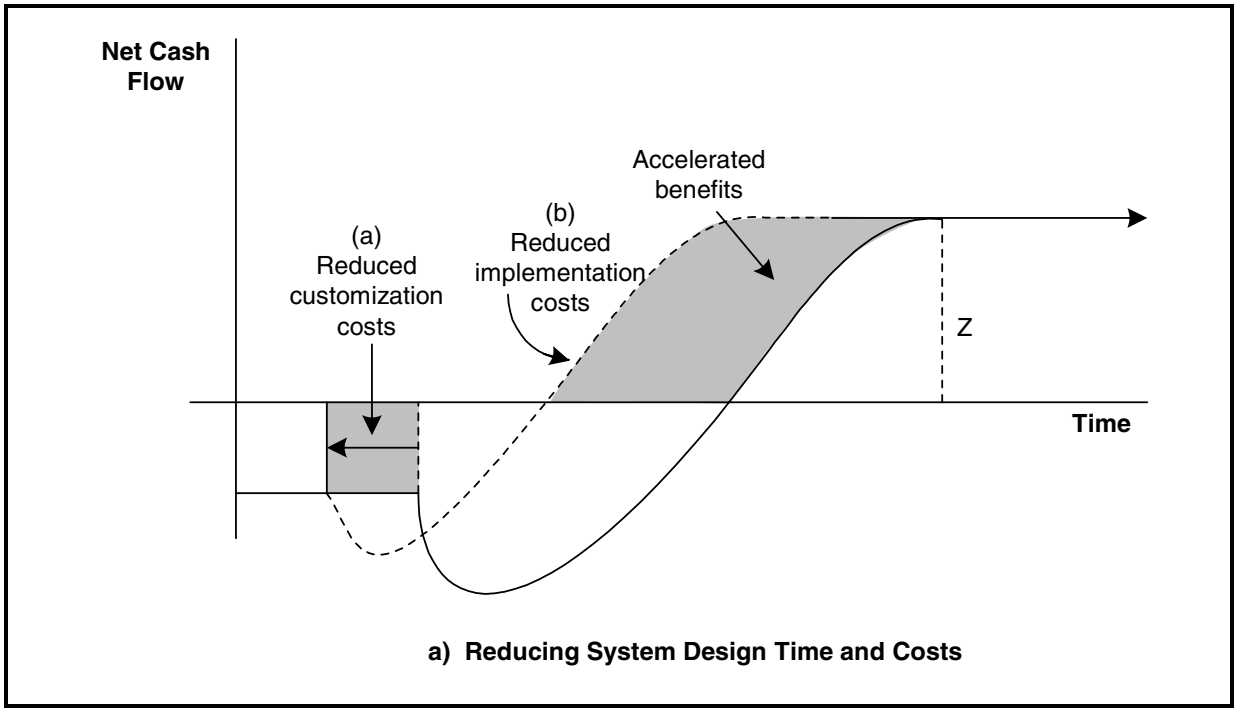
Once fully implemented, the organization using RBAC is said to be in the operations phase. At this point, the benefits (relative to alternative access control systems) include reduced administrative costs, decreased worker downtime as they are assigned new privileges, and fewer and less severe security violations. Access activities in this phase include moving users in and out of roles and defining new roles as needed. Figure 4-1 shows these benefits, Z, as a steady flow over time.

The potential impact of NIST on users' costs and benefits is shown in Figure 4-2. In Figure 4-2, NIST's contributions have

(a) reduced customization costs and time: These cost reductions are shown by the shaded square area. Time reductions are shown as a shift in the curve to the left.

(b) reduced implementation costs and time: The cost reductions are reflected in the nonparallel shift in the implementation stage.

Figure 4-2. Reducing End-User System Customization and Implementation Costs and Time



Combined, the two time reductions shift the entire life-cycle curve to the left by time "t" resulting in the acceleration of benefits shown in the second shaded area.[1] Note that the cost and time effects presented in Figure 4-2 are not mutually exclusive. Lowering the "pull" costs associated with the system customization and implementation of RBAC can contribute to the acceleration of adoption (not explicitly illustrated in Figure 4-2). It should also be noted in Figure 4-2 that the magnitude of the benefit in the

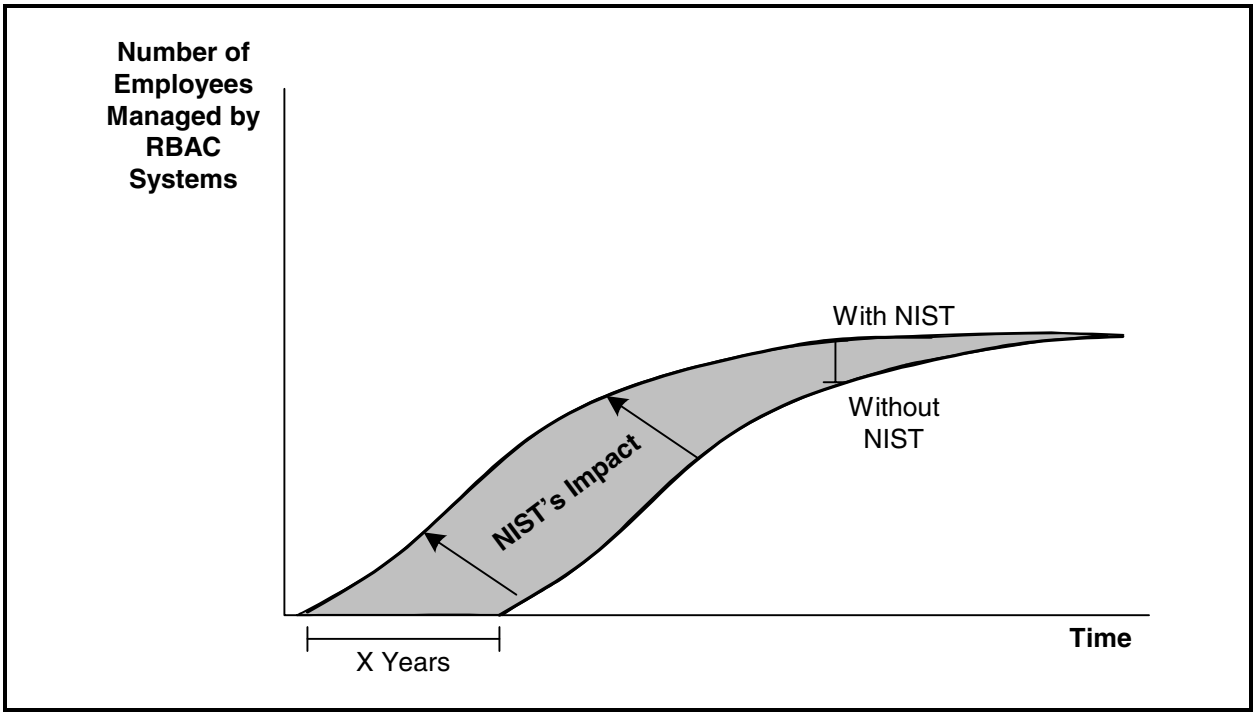
[1] For simplicity, this discussion ignores the "time value of money" effect due to the acceleration of both the costs and benefits. However, as described in Section 4.4, this factor is accounted for in the actual calculation of impact estimates through the appropriate discounting.

operations stage (Z) remains constant. During preliminary interviews with industry experts, all agreed that NIST's contributions did not have an impact on the attributes or functionality of the final RBAC systems installed. Hence, for data collection and impact estimation we assumed that product quality remains constant and focused our investigation on cost and acceleration impacts.

4.2 DIFFUSION OF COMMERCIAL RBAC PRODUCTS—INDUSTRY-LEVEL ADOPTION

Figure 4-3 illustrates the adoption of RBAC systems over time. The vertical axis indicates the cumulative share of adoptions through a given year, and the horizontal axis is time. Adoptions are measured in terms of the percentage of employees within a given industry that are being managed using an RBAC system at any given time.

Figure 4-3. End-User Adoption of RBAC Products and Services



Because adopting an RBAC system is not a discrete event and employees are brought on line over time, the penetration of RBAC is modeled as a continuous diffusion curve. The S-shaped diffusion

curve approaches the full industry potential asymptotically. The industry potential reflects the percentage of employees that are likely to be managed by RBAC systems once the full set of RBAC functionalities is made available to and adopted by industry.[2] For most industries the long penetration is expected to be close to 100 percent (i.e., some form of RBAC will be used by virtually all companies). For other industries RBAC may not be cost-effective in the near future given the current state and cost of technology.

Forecasting RBAC's rate of diffusion is difficult because it is in the early stages of adoption. It is a function of the number of current adopters, the number of potential adopters, and the rate at which information and knowledge pass from one agent to another. This study forecasts diffusion using an S-shaped logistic curve. This model is theoretically consistent with most empirical studies of technology adoption (Geroski, 2000; Mahajan and Peterson, 1985; Martin et al., 1998). Originally, only a small number of firms adopt this technology. As more firms observe the benefits realized by initial adopters, they too adopt the technology.

Forecasts of the diffusion of the technology and the total market size vary by industry and are based on interviews with experts in the industry. As shown in Figure 4-3, the impact of NIST's contributions on the development of RBAC is shown as accelerating overall adoption by X years. Note that our discussions with industry experts indicated that NIST has not influenced the quality of RBAC, only the timing of adoption. Thus, the total industry potential that the curve approaches asymptotically remains unchanged.

As mentioned above, it is likely that adoption rates and NIST's impact on these rates will vary by industry. In addition, it is likely that larger companies will adopt early and smaller companies adopt later because the benefits that large firms receive will be relatively larger. To account for variations in company size over time, we focus our empirical estimates on companies with more than 500 employees. Industry experts said that these large companies are where RBAC systems are most likely to be implemented in the near

[2]This may occur through implementing all of the NIST model features in commercial products or the full dissemination of information and tools to support in-house development.

future because larger companies realize a higher rate of return to their investment.

4.3 SUMMARY OF IMPACT HYPOTHESIS AND COST METRICS

Prior to collecting data to quantify the economic impact of NIST/ITL's RBAC project, we developed a series of impact hypotheses and cost metrics to be investigated during the interviews with industry experts. These impact hypotheses and technical and economic metrics are separated into two general categories:

- What are the benefits of RBAC relative to the counterfactual of alternative access control technologies?
- What impact has NIST had on the cost and timing of the development and adoption of RBAC and RBAC-enabled products and services?

4.3.1 The Benefits of RBAC

The counterfactual for measuring the benefits of RBAC is the use of an alternative access control system such as an ACL, DAC, or MAC. Table 4-1 lists the specific hypotheses that were investigated along with technical and economic impact metrics used to quantify each hypothesis. Table 4-1 also provides the unit by which the frequency of benefits is determined. We aggregated and normalized the benefits listed in Table 4-1 to develop an estimate of the average benefit per employee for each industry included in the analysis.

For the administrative and productivity benefit hypothesis, we used a "bottom up" estimation approach. For each of these areas, the impact is the change in labor time that is then linked to the employee's labor rate ($/hour).

To evaluate the potential economic impact of RBAC on the frequency and severity of security violations, we first asked companies what they would be willing to pay to totally eliminate security violations; then we asked about the share of violations RBAC can potentially eliminate. A "top down" estimation approach is more appropriate for investigating security violations because of the difficulty in eliciting specific information on the

Table 4-1. Benefits of RBAC Relative to Alternative Access Control Technologies

Hypothesis	Impact Metric	Cost Metric	Unit Scaling Factor or Weight
RBAC reduces administrative processing time	1. Change in administrative time for assigning existing privileges to new users (minutes)	Fully loaded administrative labor rate per hour	Number of new hires per year
	2. Changing existing users' privileges (minutes)	Fully loaded administrative labor rate per hour	Number of internal job changes per year
	3. Establishing new privileges to existing users (minutes)	Fully loaded administrative labor rate per hour	Number of new job functions
	4. Terminating privileges	Fully loaded administrative labor rate per hour	Number of employee terminations per year
RBAC increases productivity	1. Decreased downtime for new employees (days)	Percentage loss in productivity × average hourly new employee labor rate	Number of new hires per year
	2. Reduced time for upper management (minutes)	Fully loaded upper management labor rate	Number of new hires per year plus internal job changes per year
	3. Enhanced organizational structure	Investigated qualitatively	
RBAC reduces the frequency and severity of security violations	1. Elimination of security violations	Willingness to pay for eliminating security violation	Percentage of violations that can be eliminated by RBAC

number and cost of security violations from individual companies. We found that for a variety of marketing and confidentiality reasons companies are reluctant to discuss the frequency or severity of past violations. As discussed in Section 5, we relied heavily on secondary data to assess the benefits associated with security violations.

4.4 NIST'S IMPACT ON THE DEVELOPMENT AND ADOPTION OF RBAC PRODUCTS AND SERVICES

As illustrated in Figure 2-6, preliminary interviews with NIST and industry experts indicated three main pathways through which NIST's contributions affect the development and adoption of RBAC products and services:

- lowering the costs of R&D, including system design and software development;
- lowering implementation costs, including role definition and migration from previous systems; and
- accelerating the realization of benefits, described in Table 4-1, of RBAC relative to alternative access control systems.

These hypotheses are listed in Table 4-2 along with the technical and economic impact metrics. Preliminary discussions with industry experts indicated that virtually all the R&D and implementation costs are in the form of staff time. Thus, the technical and economic impact metrics for the first two hypotheses are labor in terms of changes in labor hours and labor expenditures, respectively. Changes in R&D expenditures per company were averaged and then weighted by the number of software companies developing RBAC products and large companies developing in-house RBAC systems.

The technical and economic impact metrics for NIST's acceleration effect are the average number of months an adoption decision was advanced and the value of the benefits of RBAC realized as a result of the acceleration. Benefits were calculated on an annualized per-employee basis and then weighted using the shift in the diffusion curve as shown in Figure 4-2.

Finally, it should be noted that preliminary interviews with industry experts indicated that NIST's activities will probably ***not*** change the long-run "quality" of RBAC products and services, only the cost of development and the timing of availability and adoption. Hence changes in the magnitude of annual benefits per employee and the long-run industry penetration of RBAC systems are not included as impact hypotheses attributable to NIST. Industry experts said that the attributes and features included in the NIST RBAC model would

Table 4-2. NIST's Impact on Commercial RBAC Products and Services

Hypothesis	Impact Metric	Cost/Benefit Metric	Unit Scaling Factor or Weight
NIST's activities have lowered the private cost of developing RBAC products and services	1. Change in R&D labor hours for software developers of commercial products	Reduced R&D labor expenditures per software company	Number of software companies developing RBAC products
	2. Change in R&D labor hours for in-house development by users	Reduced R&D labor expenditures per in-house development	Number of in-house implementations by users
NIST's activities have lowered the private cost of implementing RBAC systems	1. Reduced implementation time and labor effort	Reduced implementation costs per employee	Industry adoption of RBAC in terms of number of employees
NIST's activities have accelerated the availability adoption of RBAC products	1. Number of months NIST accelerated the availability of RBAC products (i.e., shift in the diffusion curve)	Realization of benefits (and costs) per employee described in Table 4-1 sooner	Acceleration of the number of employees in each industry managed using RBAC
	2. Number of months NIST accelerated the adoption of RBAC products by end users (i.e., shift in the diffusion curve)	Realization of benefits (and costs) per employee described in Table 4-1 sooner	Acceleration of the number of employees in each industry managed using RBAC

Note: Preliminary interviews with industry experts indicted that NIST's activities have ***not*** influenced the "quality" of RBAC products and services, only the cost and timing. Hence the size of annual benefits and the overall industry penetration of RBAC systems are not included as impact hypotheses.

have likely been developed by industry in the absence of NIST, however at a later time and with greater costs.[3]

The exclusion of RBAC "quality" changes attributable to NIST is a conservative assumption in that it leads to lower bound estimates of the economic impact of NIST's RBAC project. It is very possible that NIST's contributions to the development and standardization of the higher levels of RBAC will accelerate the use of hierarchy and constraint features in RBAC products. However, because software vendors did not convey this information during our interviews we have not included this category in the quantitative impact estimates.

[3]Note that the quality of access control systems in general does change due to NIST, reflecting RBAC's superiority over alternative systems. The improved quality of access control systems is captured through NIST's acceleration effect on the development and adoption of RBAC.

The applicability of RBAC and the long-run market penetration of RBAC for a given industry are a function of several factors, including computer and network technologies, basic characteristics of their business operations, and future reductions in hardware costs. These findings, gathered from preliminary industry interviews, were also investigated as part of the Internet surveys and case study discussed in the following sections. The surveys and case study confirmed that it is unlikely NIST affected the long-run benefits of RBAC. However, several respondents indicated that the NIST model has affected the short-run quality of RBAC products and services available to industry. This effect is captured in our model as part of the acceleration of realized benefits.

4.5 CONCEPTUAL APPROACH TO MODELING THE ECONOMIC IMPACTS OF NIST/ITL'S RBAC PROJECT

The empirical model of the economic impact of NIST's contributions is based on the hypotheses presented in Table 4-1 and Table 4-2. From the impact and cost metrics listed in these tables, we calculated individual company-level R&D costs, normalized by the number of employees, and per-employee RBAC benefits resulting from the NIST/ITL project. These employee-level impacts are adjusted for inflation and discounted using a 7 percent social discount rate to estimate the net present value (NPV) of NIST's contributions. This is compared to the NPV of NIST's expenditures to estimate the return to the NIST/ITL project. The estimation procedure is explained in detail below.

4.5.1 Expressing the Net Benefits of RBAC

We begin by developing equations representing the net benefit of RBAC to society (excluding NIST's expenditures). This includes private R&D costs of software developers and users; customization and implementation costs by users; and benefits to users from reduced administrative processing time, increased productivity, and reduced frequency and severity of security violations.

The benefits of RBAC, as described in Table 4-1, are defined as the flow of operating benefits (OB) over time. Benefits are expressed

per employee and may vary by industry, i indexes industry, and t indexes year:

$$OB_{it} = AC_{it} + PB_{it} + SB_{it} \quad (4.1)$$

where

OB_{it} = operating benefits per employee

AC_{it} = administrative cost reductions per employee

PB_{it} = productivity benefits per employee

SB_{it} = security benefits per employee

Implementation costs are also expressed as expenditures per employee for a given industry:

IC_{it} = RBAC user customization and implementation costs per employee

Finally, RBAC R&D costs are expressed as average software developer R&D expenditures and average in-house R&D expenditures over time:

R&Dsd = total R&D costs for a typical software development company for implementing RBAC concepts into their products [4]

R&Dih = total R&D costs for a typical user for integrating RBAC concepts into their in-house systems

The time series of net benefits (NB_t) from RBAC can then be calculated by summing across the costs and benefits to software developers and users in all industries:

$$NB_t = R\&Dsd * Nsd_t + R\&Dih * Nih_t + \sum_{i} (OB_{it} - IC_{it}) * \Delta Emp_{it} \quad (4.2)$$

where

Nsd_t = number of software developers in year t that developed an RBAC product

Nih_{it} = number of users in industry i that developed in-house RBAC products in year t

Emp_{it} = number of employees in industry i being managed using RBAC systems in year t

[4] R&D costs are allocated to the initial year of RBAC system development. Industry experts indicated that NIST's impact on the development process typically occurred early in the project; hence, any impact on R&D expenditures was likely to be realized in the first year.

The net benefits are separated between the one-time development and implementation costs versus the continuing operational and administrative benefits. Note that the end-user benefits are a function of the cumulative number of employees being managed by an RBAC systems, whereas the end-user costs represent the incremental number of employees brought on to RBAC systems.

4.5.2 Modeling the Impact of NIST/ITL's RBAC Project

As described in Table 4-2, the potential economic impact of NIST/ITL's RBAC project results from changes in R&D costs, changes in implementation costs, and changes in the number of employees being managed by RBAC systems over time. This is expressed as

ΔR&Dsd	=	change in R&D costs for software developers
ΔR&Dih	=	change in R&D costs for users developing in-house RBAC systems
ΔIC_{it}	=	change in implementation costs
Δ Emp $_{it}$	=	change in the number of employees being managed by RBAC systems

Rewriting Eq. (4.2) in terms of changes resulting from NIST's contributions yields

$$\Delta NB_t = \Delta R\&Dsd * Nsd_t + \Delta R\&Dih * Nih_t + \sum^{i} [OB_{it} - (IC_{it} - \Delta IC_{it})] * \Delta Emp_{it} \quad (4.3)$$

4.5.3 Calculating Measures of Economic Return

We used the timeline of net benefits attributed to NIST and NIST expenditures to develop three summary measures of the net benefits of the RBAC project: the benefit-cost ratio, the NPV, and the social rate of return.

In the benefit-cost ratio, the numerator is the time series of ΔNB_t (Eq. [4.3]) associated with NIST's contributions, discounted back to 1994—the year in which NIST/ITL's RBAC project was initiated. The denominator of the benefit-cost ratio is the time series of NIST/ITL RBAC project expenditures in each year (C_t), also discounted back to 1994:

$$(B/C) = \frac{\sum_{i=0}^{n} \frac{B_{(t+i)}}{(1+r)^i}}{\sum_{i=0}^{n} \frac{C_{(t+i)}}{(1+r)^i}} \tag{4.4}$$

An inflation-adjusted social rate of discount of 7 percent is used to discount benefits and costs over time.

The NPV of the NIST/ITL RBAC project can be computed as

$$NPV = \sum_{i=0}^{n} \left[\frac{B_{(t+i)}}{(1+r)^i} - \frac{C_{t+i}}{(1+r)^i} \right]. \tag{4.5}$$

The social rate of return is the value of r that sets NPV equal to 0 in Eq. (4.5).

5 Primary Data Collection

To estimate the net benefits to RBAC described in Section 3 and NIST's contributions to realizing these net benefits, we collected primary and secondary data throughout the RBAC supply chain. The data collection activities focused on software developers and organizations (referred to as end users) that integrate RBAC products into their business operations.

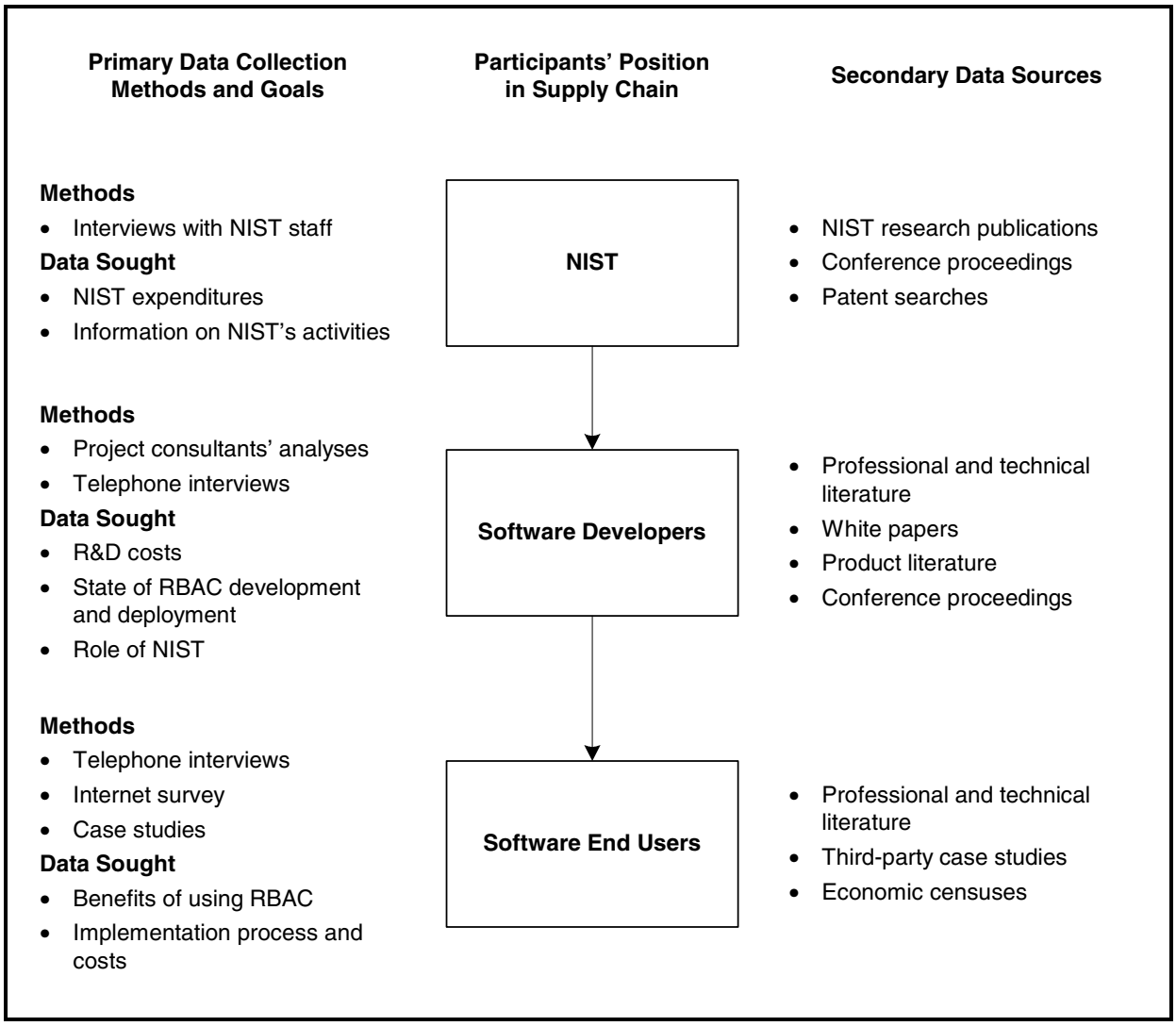
Figure 5-1 provides a conceptual overview of the primary and secondary data collection activities undertaken to support this study. Primary data collection methods included telephone interviews with software developers and end users, an Internet survey of end users, and a case study with a mulitproduct insurance company. Secondary data sources included the professional literature and economic surveys conducted by the federal government and research organizations. In this section we discuss our data collection methodologies and goals.

5.1 RBAC SOFTWARE DEVELOPERS

RTI conducted a series of detailed interviews with software developers to determine the state of the industry vis-à-vis RBAC development and deployment in commercially available products.

The software developer interviews had three goals within this larger construct. The first goal was to assess the current state of RBAC development and deployment. The second goal was to collect information on the R&D costs of integrating RBAC models into developing software products.

Figure 5-1. Overview of Data Collection



The third goal was to determine the effect of NIST's involvement in developing RBAC and products that are RBAC-enabled. Included therein was the potential to determine to what extent NIST's involvement in developing RBAC furthered its diffusion.

As part of our discussion with software developers, we also collected information to compare the costs and benefits to end users of RBAC with other access control technologies. This information supported the development of the end-user surveys.

5.1.1 Software Developer Population and Interview Methodology

We conducted detailed telephone interviews with eight software developers. We used three information sources to identify prospective participants for the developer survey: conference proceedings, technical literature, and word of mouth. Several professional societies sponsor workshops and conferences on the security and audit of information systems. RTI obtained the attendance lists and conference proceedings from several recent RBAC conferences and workshops. We also searched the professional and technical literature for authors of recent articles on the subject. Once the actual interviews began, several participants suggested that we contact others if the participant was unsure about a question or if the participant thought a colleague would be able to contribute additional insights to the study.

The software developers RTI contacted represented both academia and private enterprise (see Table 5-1). We did not contact all of the individuals for whom we had contact information; rather we selected those individuals whose body of work complemented and set them apart from the rest of the list. The eight software developers that were formally interviewed are among the most active in the field, as indicated by their conference attendance, number of articles in the professional and technical literature, number of corporate white papers authored, and participation in formal societies. Interviewees represented professors, systems administrators, and product managers as well as both executive and technical staff.

Each interview was conducted over the telephone and lasted between 45 and 90 minutes. Participants were provided with a copy of the interview guide and a memorandum outlining the project's goals before the actual conversation. If after each initial interview further clarification about any particular comments or issues raised was needed, we recontacted the interviewee.

In addition, several developers contacted were unavailable for lengthy discussions; however, they did agree to speak briefly over the telephone and discuss their development plans and general industry trends. Although no quantitative information was obtained, these short conversations did confirm the comments and insights gathered from the eight formal interviews.

Table 5-1. Interviewed Software Developers' Background
The software developers represent a variety of organizations, but they share the common trait of being involved in the research and development of RBAC models and products.

Software Developer	Affiliation	Background
Software Developer 1	Corporate	Product development manager
Software Developer 2	Academic	University professor
Software Developer 3	Corporate	Product development manager
Software Developer 4	Academic and corporate	Systems administrator and programmer; Ph.D. candidate
Software Developer 5	Corporate	Research and development scientist
Software Developer 6	Corporate	Research and development scientist
Software Developer 7	Corporate	Vice president of product development
Software Developer 8	Corporate	Product development manager

5.1.2 Topics Covered in the Software Developer Interviews

RTI asked software developers to reflect on the costs and benefits of RBAC, its current and potential market penetration, and NIST's role in development and adoption. The developer questionnaire consisted of six sections, each containing a series of short-answer and table-format questions. Appendix A contains a copy of the survey. The first section asked for some background information on the industry and size of the firm. The remaining sections asked about the following:

- Market Penetration of RBAC: The questionnaire began by asking developers some basic questions about their company's software products and/or research interests and their customers.
- Future Technology Improvements: This section asked about the how future improvements in both role-based and nonrole-based access models might change those technologies in the future and to what extent.
- Software Development: Developers were also asked about their timeframe for incorporating RBAC into their products and their research and development costs. They were also asked whether articles in the professional literature facilitated RBAC's inclusion.
- NIST's Contributions to the Development of RBAC: Developers were asked to what extent, if any, NIST's research into RBAC influenced the research and development of their products and the market for role-based products.

The survey instrument contained in Appendix A was used primarily as a discussion guide. It was shared with respondents prior to the interviews and served as the general structure for the discussions. However, in many cases it was the unanticipated information and comments obtained during the interviews that proved most insightful.

5.2 RBAC SOFTWARE END USERS

RTI conducted an Internet survey of security administrators sent to subscribers of *Information Security Magazine,* a leading trade publication for information and systems security administrators. Ninety-two administrators responded to the survey. The Internet survey's goals were

- to determine the administrative costs of establishing and changing user profiles when RBAC or other access control technologies are used;
- to determine the frequency of security violations, both internal and external, when RBAC and other access control technologies are used; and
- to determine the difficulty of altering or changing access control systems.

We also conducted telephone interviews with one major telecommunications firm and a large commercial bank. Although these interviews yielded little quantitative data, they were integral to understanding the benefits and implementation costs of RBAC. The information gathered from these interviews helped define the benefits and costs categories in Section 2.

5.2.1 Internet Survey Population and Methodology

We sent an e-mail message on December 19, 2000, to 9,530 of the magazine's subscribers to tell them about the survey and request their participation. The e-mail message was targeted to magazine subscribers who indicated they were responsible for network and systems security administration. It directed the recipient towards the RTI web page that housed the survey.

Ninety-two individual companies responded to the e-mail and completed some portion of the Internet survey. Although the overall response rate is low, this response rate is consistent with previous studies using this database of subscribers. Respondents

were given the option to skip questions they did not wish to answer.

Because the magazine's subscriber base is not limited to any particular industry, we anticipated that companies that responded to the survey would represent an array of industries. One-third of the companies were in the information technology industry, a category that includes software and information consulting firms as well as hardware manufacturers (see Table 5-2). The end-user discussion included in Section 2 indicates that key implementers of RBAC are likely to include financial institutions and health care organizations. These two industries make up the second and third largest industry categories, a further indication that RBAC has generated a significant amount of interest in these areas.

Table 5-2. End-User Internet Survey Respondents by Industry
Information services accounted for over one-third of respondents, with finance and health care organizations accounting for approximately another third.

Industry	Percentage of Respondents
Information[a]	42%
Finance and insurance	20%
Health care and social assistance	14%
Government	9%
Educational, professional, scientific, and technical services	5%
Manufacturing	4%
Utilities	3%
Transportation and warehousing	3%
Total	100%

[a]Includes telecommunications.

5.2.2 Topics Covered in the Internet Survey

The Internet survey asked systems administrators to reflect on the access control policies and procedures used within their respective companies' corporate information systems and intranet. The survey consisted of six sections, each containing short-answer and table-format questions. Appendix B contains a copy of the survey. The first section asked for some background information on the industry and size of the firm. Other sections asked about the following:

- Access Control Technologies Used by Your Firm: The first portion of the survey asked about the respondents' current and previous access control technologies and products.
- RBAC System Design: If companies had designed their systems in-house, they were asked about development time, costs, and whether they were successful. Companies that purchase RBAC systems were asked whether they were aware of RBAC before the purchase and why they chose not to design a system in-house.
- RBAC System Implementation: In this section, administrators answered questions related to the amount of time it took to implement the system, the number of employees managed using the system, and if other costs were incurred to support the migration.
- The Benefits and Costs of Maintaining RBAC Systems: This section asked for labor-hour estimates for a series of systems administration tasks and for comparisons between RBAC and non-RBAC technologies.

5.3 A CASE STUDY OF AN RBAC END USER

To complete our overview of the state of RBAC in the marketplace, RTI conducted an end-user case study. The case study more deeply explores the impact RBAC has on organizations that use it. The case study differs from the Internet survey of systems administrators by focusing on systems migration and operations transitions. RTI identified those individuals who are involved in both the management decisions related to RBAC and the systems migration and integration process. Before the interview, each contact was provided with background information on the project and NIST and a list of discussion topics. RTI held conference calls and later followed up with one or two short emails and phone calls. A discussion of each case study follows in Section 5.

6 RBAC Case Study: Multiline Insurance Company

As part of the data collection process, RTI conducted a case study of a company implementing RBAC. One of the primary goals of the case study was to learn more detail about the RBAC implementation process than can be gathered in one 30- to 45-minute telephone interview. The case study was also an opportunity to more fully explore the benefits and costs of RBAC from the vantage point of a software end user.

RTI conducted the case study with a multiline insurance company (herein referred to as "the Company"). RTI selected the Company for the case study for two principal reasons. First, the Company is implementing RBAC to manage both its employees' access permissions and its extranet users' permissions. The case study was able to capture, with one software end user, insights from implementing RBAC in these two environments. Second, because the Company's extranet users are contracting agencies, the case study would also capture insights related to delegated administration and other functionalities afforded RBAC users.

This section discusses the Company's line of business and how the Company intends to leverage RBAC to enrich its business model and improve employee productivity. The installation and implementation will cost the Company an estimated $783,636 over the course of 12 to 18 months. Once fully implemented, however, RTI estimates that the annual administrative and productivity estimates will total nearly $661,330. In addition, the Company

estimates that its RBAC-enabled e-business strategy will increase its annual amount of new business by 10 to 20 percent.

6.1 RBAC IMPLEMENTATION BACKGROUND

The Company's primary line of business is the provision of an array of insurance products, including home, auto, business, and life insurance. Like many multiline insurers, the Company does not sell directly to policyholders, but it instead teams with locally operated independent insurance agents. These local insurance agents market and sell products within their area, contracting with the Company upon selling a policy. The Company's annual revenues are measured in the billions, it has several thousand employees, and it works with hundreds of agencies located across the U.S.

The Company expects that using RBAC will increase productivity and increase its amount of new business annually. RBAC will also provide the level of security required by an institution with a large number of users and a wide variety of user types, including potentially competing insurance agents.

The Company is in the middle of rolling out RBAC to its internal and external user population; the rollout is occurring in two stages. First, the Company is providing electronic services to its customer base, the local insurance agencies, via the Internet. The system will use RBAC to provide systems security and to relieve maintenance and administrative pressures by delegating administration. As this process nears completion, the Company will devote more resources to its internal migration from identity-based ACLs to RBAC.

The Company expects that using RBAC will increase productivity and increase its amount of new business annually. RBAC will also provide the level of security required by an institution with a large number of users and a wide variety of user types, including potentially competing insurance agents. The Company was not able to provide any quantitative information concerning security benefits; however, it openly discussed the other benefits it expected to accrue and costs it expected to incur. These costs and benefits, quantified by RTI, are presented in Table 6-1.

6.2 BENEFITS OF USING RBAC TO MANAGE EXTRANET USERS

The Company's client base consists of hundreds of independent insurance agencies located across the U.S., each employing approximately three agents and their support personnel. Traditionally, insurance agents interacted with the Company

Table 6-1. Summary of the Company's Costs and Estimated Benefits
The Company's strategy should save it at least $661,330 annually, but to reap these benefits it must first outlay $783,636 in labor, software, and hardware expenses.

Variable	Dollar Value	Economic Metric
Enhanced organizational productivity	$471,040	Reduced paper- and telephone-based workload for insurance claims and policy-processing professionals.
Delegated administration of extranet user accounts	$161,086	Avoided cost of corporate systems administrators maintaining extranet users' accounts.
Reduction in new employee downtime	Undisclosed	Reduction in the amount of time an employee is without access permissions.
Improved management of employees' permissions using RBAC	$29,204	The cost difference between RBAC and non-RBAC policies to manager employees' user accounts.
Total Annual Benefits	**$661,330**	
Software expenses	$120,000	Software purchases, including maintenance and support agreements.
Hardware expenses	$20,000	Hardware purchases to support systems migration and e-business strategy.
Consulting fees	$24,000	Fees paid to consultants to assist in the implementation process.
Labor expenses	$608,088	Labor expenses of employees tasked with implementing RBAC systems and e-business strategy.
Role engineering expenses	$14,548	Labor expenses related to determining the characteristics of roles to be used.
Total One-time Costs	**$783,636**	

through telephone calls and written communication. Agents contact the Company directly to determine rates, receive quotes, and obtain other information. After receiving information from the Company, agents then recontact prospective policyholders to inform them of the results. The process of contacting the Company directly to determine rates and to gather other information translated into a significant amount of time between a customer's inquiry and the sale of the policy. If the customer should choose to purchase the policy, the agent must then initiate a process whereby the policy is enacted and the appropriate forms were filed at the agency and mailed to the Company. The Company would supplement its records with information obtained from agents in the additional mailings and other communications. The process of

completely selling a policy, including mailing and final data entry, could take as long as 4 to 6 weeks.

Delegated administration of the Company's agents is expected to decrease the systems administrator's workload by approximately 1.5 fulltime employees annually, compared to using an alternative access control model.

RBAC is the technology enabling the Company's strategic e-business initiative. The RBAC software will grant or deny access to users to data and applications as users' roles dictate. In essence, the software is the platform to which data and applications will be linked. Agents will interact with the Company over the Internet. Agents will be assigned roles that allow them to enter policyholder information, examine rates, and sell products instantly to customers. The goal is to allow agents to maintain, access, determine, and interact with policy information and details electronically. The Company also estimates that the ability to instantly register and sell products to prospective policyholders will increase its amount of new business by 10 to 20 percent annually.

The Company could have selected an alternative access control model, but it would have been more costly, although the extent of the additional cost is unknown. What is known, however, is that a non-RBAC solution would have entailed a larger programming component, which would have increased installation and customization costs. The system would also have been far more costly to operate and less secure for several reasons related to systems administration and maintenance, such as user directory maintenance and user account maintenance (i.e., no delegated administration).

6.2.1 Simplifying Systems Administration and Maintenance

The company will use RBAC's delegated administration capability to establish an administrator at each agency who will be tasked with performing the basic systems administration and role maintenance for its agency. It will take the Company less than 1 hour per agency to establish administrators and set up the basic structure, a cost that is included in the labor cost estimates presented in Section 6.4. Delegated administration of the Company's agents is expected to decrease the systems administrator's workload by approximately 1.5 full-time employees annually, compared to using an alternative access control model. The Internet survey uncovered that the average, fully loaded wage of systems administrators performing these functions is

approximately $51.62 per hour.[1] At this wage, the Company would save $161,086 annually.

Delegated administration does not push costs further down the supply chain, rather there may be benefits to those organizations to which account administration has been delegated. For example, the cost of having the office manager at a local insurance agency assign a role to a new agent may be outweighed by the benefit of that agent having his or her permissions quickly. If the office manager does not have to arrange account set-up and administration with the Company, he or she avoids the labor and lag time expenses. The agent is also able to assume his or her regular duties.

6.2.2 Enhancing Organizational Productivity

Policy and policyholder information is transmitted to the Company securely over the Internet, reducing the Company's administrative and data entry burden as well as the amount of paper circulating among its departments. The Company currently employs 40 people tasked solely to maintain the communication and data entry associated with managing relationships with agents in the mailroom, call center, support, and data entry departments. It estimated that the new initiative will make available about 20 percent of their time. Based on information gathered from the Bureau of Labor Statistics, the mean national loaded wage for insurance claims and policy processing clerks is estimated to be $29.44 per hour.[2] The e-business strategy should free up 16,000 person-hours annually, given its current level of employment. The value of those hours is therefore at least $471,040.

---

[1] According to the 2000 National Occupational Employment and Wage Estimates published by the Bureau of Labor Statistics, the mean wage for network and computer systems administrators is $25.81 per hour, or $53,685 annually. This estimate was multiplied by 2.0 to estimate the additional cost to the employer for employee benefits, such as employer-sponsored health and dental insurance and 401(k) contributions, as well as administrative and overhead costs.

[2] According to the 2000 National Occupational Employment and Wage Estimates published by the Bureau of Labor Statistics, the mean wage for insurance claims and policy processing clerks is $14.72 per hour, or $30,618 annually. This number was multiplied by 2.0 to estimate the additional cost to the employer for employee benefits, such as employer-sponsored health and dental insurance and 401(k) contributions, as well as administrative and overhead costs.

6.3 BENEFITS OF USING RBAC TO MANAGE EMPLOYEES (INTRANET USERS)

The Company is replacing its current, identity-based access control system with a role-based one. The Company employs a few thousand people at several offices. IT systems administrators at the headquarters facility currently maintain each employee's access permissions using ACLs. The Company estimates that once it implements RBAC its principal benefits will fall into two categories: reduced new employee downtime and simplified systems administration and maintenance.

6.3.1 Reduction in New Employee Downtime

The administrative benefits of allowing a new employee to quickly assume his or her duties by having access permissions more quickly are potentially substantial. Being a large insurer, the Company has scores of employees in similar job functions. With RBAC, it can create and define a role once and then assign that role to new employees as opposed to adding the employee's user ID to each ACL. The Company indicated that the time until a new employee is fully enabled is currently 2 to 3 days, including the routing of paperwork. The role-based system and accompanying administrative policies are expected to reduce the amount of time significantly; therefore, the employee is able to access data and applications more quickly.

Because information on employee turnover and employment at the Company is confidential, we do not present the impact estimates. However, if we assume that the amount of downtime is reduced by one-half, and that during that time the employee is 85 percent productive, we can estimate what the approximate benefits are. For a new policy-processing clerk, the reduction in new employee downtime would be worth $44.16.[3] This number is excluded from the total benefits calculation for the Company case study because it is meant solely to illustrate the benefit.

[3]The reduction in downtime (50% of 2.5days = 1.25 days = 10 hour) is multiplied by the loaded wage rate for policy-processing clerks ($29.44 per hour) and the productivity loss (15%).

6.3.2 Simplified Systems Administration and Maintenance

It is estimated that using RBAC rather than identity-based ACLs to manage user permissions will save the Company $29,204 annually.

As explained in Section 2, the Company expects that the ability to more quickly assign access privileges will reduce its systems administration and maintenance costs. The time that otherwise would have been spent determining and assigning privileges will be free for other tasks. Alternatively adjusting or terminating privileges for employees that are either leaving the company or moving to new positions internally will be equally facilitated. The aggregate effect is an improvement in administrators' productivity. It is estimated that using RBAC rather than identity-based ACLs to manage user permissions will save the Company $29,204 annually.[4]

6.4 RBAC IMPLEMENTATION COSTS

The migration to RBAC and the implementation of the e-business strategy will cost the Company approximately $784,000. The labor costs associated with installation as well as the software and hardware costs are one-time costs. The Company will intermittently incur role engineering costs as its business activities warrant redefining roles over the life of the system. The Company's total user population is expected to be 10,000; thus, the implementation cost per user will be approximately $78.36.

6.4.1 Software and Hardware Expenses

The Company's costs included software and hardware purchases, consulting fees, and labor expenses. The access control software, which complements the e-business platform and other software, cost the company $120,000, including a 1-year maintenance and support agreement. The Company also hired consultants to assist in the implementation at a cost of $24,000. It purchased two additional servers to facilitate the migration and to support the e-business initiative at a total cost of $20,000. Thus, the Company's total software and hardware outlay totaled $164,000.

[4]Results from the Internet allowed RTI to calculate the number of minutes administrators save by using RBAC rather than other access control models. The Internet survey also yielded data concerning the average number of times administrative tasks such as assigning and terminating permissions were performed annually. Using these national averages, we were able to estimate the impact to the Company. Section 6 more fully discusses the time-savings estimates and administrative activities estimates.

6.4.2 Systems Administrators' Labor Expenses

Three computer systems managers are tasked full time to accomplish both the e-business and RBAC rollout to independent agencies and the internal RBAC rollout. These systems managers anticipate that the entire process will take between 12 and 18 months. Included in these costs are several tasks such as

- software customization,
- programming related to web-enabling applications,
- software and hardware installation,
- training and education,
- defining roles within the software package, and
- all other labor activities related to the software rollout.

Using data provided by the Bureau of Labor Statistics, we estimated the loaded wage rate of computer and information systems managers to be $77.96 per hour.[5] The midpoint of the Company's time horizon and the number of administrators tasked yield an estimated labor expense of $608,088.

6.4.3 Role Engineering Expenses

The final labor activity to be included is role engineering. The Company has yet to complete the role engineering process and is unsure of the amount of time, and therefore the expense, it will take to complete the task. The Company anticipates that several more meetings in the coming months will be required to determine and establish administrative policies and roles and to work out organizational issues. Role engineering is an iterative process and the Company will most likely revisit role definitions established during initial rollout.

[5] According to the 2000 National Occupational Employment and Wage Estimates published by the Bureau of Labor Statistics, the mean wage for computer and information systems managers is $38.98 per hour, or $81,078 annually. This number was multiplied by 2.0 to estimate the additional cost to the employer for employee benefits, such as employer-sponsored health and dental insurance and 401(k) contributions, as well as administrative and overhead costs.

The role engineering cost is also a recurring cost, particularly as the Company grows and its organizational structure shifts.

The role engineering cost is also a recurring cost as the Company grows and its organizational structure shifts. New tools and experience with role engineering should make the process less costly in the future. However, it is impossible to hypothesize how the Company's future business environment may affect the need to redefine the roles established during the rollout. For this case study we assumed that role engineering is a one-time cost and that the organizational structure of the Company is fixed.

At the time the interviews were conducted, the Company had held 40 hours of meetings, each with an average of five individuals consisting equally of general managers and computer and information systems managers. The loaded wage rate of computer and information systems managers is estimated to be $72.74.[6] Using the wage rates for these two groups of employees, we calculate the cost of these meetings to be $14,548.

6.5 TIME SERIES OF BENEFITS AND COSTS

The RBAC software and model will be in place indefinitely. Because of the significant capital and labor expense of implementing access control policies and products, it is unlikely that the Company will migrate to an alternative model in the foreseeable future. It may deepen or adjust the model it has chosen, which may include further labor and capital investment for software revisions or the creation of new roles or redefinition of existing ones. At present the Company has no plans to deepen or adjust its model once RBAC has been fully deployed.

Table 6-2 presents a time series of the Company's estimated costs and benefits, based on its current expenditure plans. The time series assumes that real wage rates are constant and that the Company's organizational structure remains fixed. All dollars are 2001 dollars.

[6] According to the 2000 National Occupational Employment and Wage Estimates published by the Bureau of Labor Statistics, the mean wage for general and operations managers is $33.76 per hour, or $70,220 annually. This number was multiplied by 2.0 to estimate the additional cost to the employer for employee benefits, such as employer-sponsored health and dental insurance and 401(k) contributions, as well as administrative and overhead costs..

Table 6-2. Time Series of the Company's Costs and Benefits
The Company's costs are spread over six quarters encompassing three calendar years. Because some employees will be managed using RBAC while others are being migrated to the new system, costs and benefits overlap. The total estimated annual benefit to the Company is not first accrued until 2003.

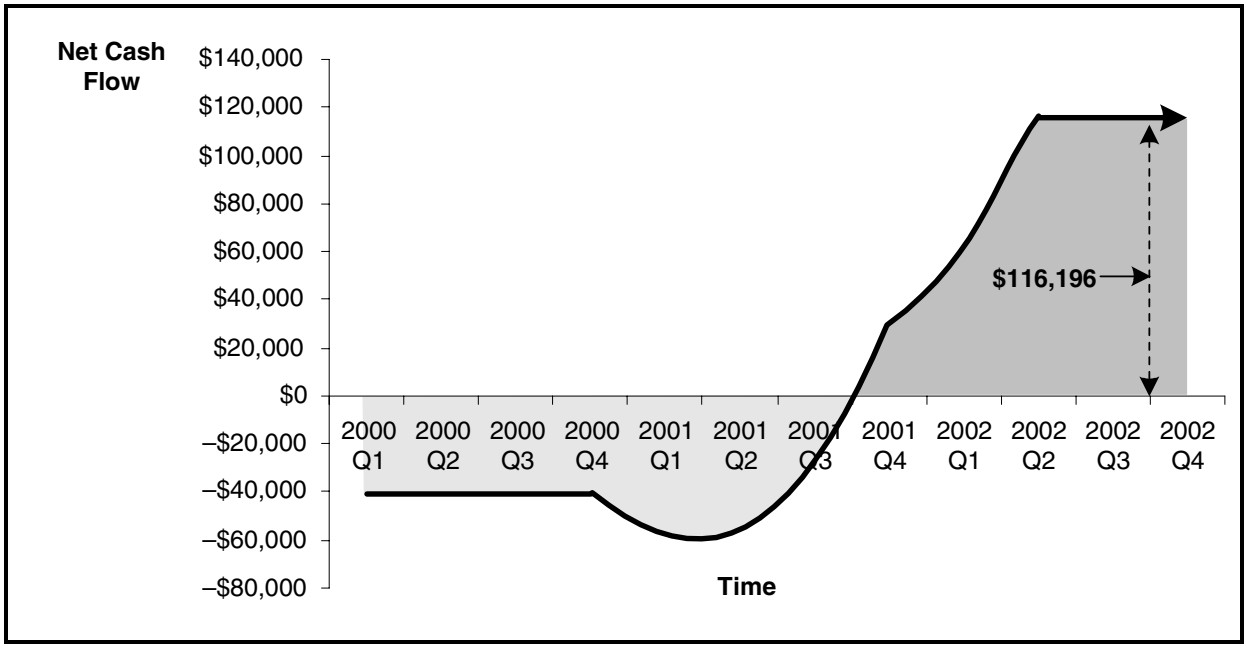
Year	Costs	Benefits
2000	$164,000	
2001	$501,018	$159,857
2002	$121,618	$659,505
2003		$661,330
2004		$661,330
2005		$661,330
2006		$661,330

Expenses are distributed over a six-quarter period. The Company purchased the hardware and RBAC software during the final quarter of 2000. The time series assumes the Company began implementation at the start of the first quarter of 2001 and completed it 15 months later at the end of the first quarter of 2002. Hence, there was a one-quarter lag between software and hardware purchases and the beginning of implementation. The role engineering process was completed before users were migrated to the new system; therefore, the implementation labor expense is distributed evenly over the 5-quarter period, but the role engineering expense was limited to the first two quarters.

The Company plans to first bring its extranet users into the system and then its employees. The entire process will take 9 months; during 3 months both extranet users and employees will be migrated. The process began in the third quarter of 2001 and will be completed at the end of the first quarter of 2002. Although some benefits will be accrued in 2001, the total estimated annual benefit does not begin to accrue until 2003.

Figure 6-1 illustrates the net benefits to the Company on a quarterly basis. Although the software and hardware costs were incurred solely during the fourth quarter of 2000, Figure 6-1 conceptualizes these particular costs over the entire 2000 calendar year. This adjustment was made because the labor costs were distributed

Figure 6-1. Quarterly Flow of Net Benefits
This figure conceptually illustrates the flow of the Company's net benefits on a quarterly basis from implementation to full operation.



evenly over time, when in reality some months may have seen more labor activity than others. If the software and hardware costs had been depicted as a spike in net cash flows, the resulting data point would have made the curve's cost area difficult to illustrate and understand.

7 Survey Findings and Estimation of Impact Metrics

This section summarizes the findings from the data collection activities in terms of the impact metrics and benefit equations defined in the Section 3. These metrics will be used to develop the time series of changes in benefits and costs resulting from NIST's activities presented in the following section.

The Internet survey, telephone interviews, and end-user case study yielded a large amount of quantitative data on the benefits and costs of developing, implementing, and using RBAC and RBAC-enabled products and services from both the software developer and end-user perspectives. In this section we discuss

- ➤ quantified end-user benefit and cost metrics,
- ➤ R&D costs associated with developing RBAC products and services,
- ➤ the current and projected diffusion of RBAC and RBAC-enabled products, and
- ➤ NIST's impact on the development and adoption of RBAC.

7.1 QUANTIFIED END-USER BENEFIT AND COST METRICS

We used the metrics described in Table 3-1 (repeated in Table 7-1 for convenience) to estimate the benefits of RBAC to end users. In addition to benefits, we estimated the costs borne by end-user companies associated with customization and implementation. We

Table 7-1. End-User Benefits of RBAC

Hypothesis	Impact Metric
RBAC reduces administrative processing time	1. Change in administrative time for processing a new employee (minutes) 2. Change in administrative time to revise privileges for job reassignment (minutes) 3. Change in administrative time to terminate privileges (minutes)
RBAC increases productivity	1. Decreased downtime for new employees 2. Reduced time for upper management 3. Enhanced organizational structure
RBAC reduces the frequency and severity of security violations	1. Elimination of security violations

then normalize the average end-user benefits and costs by company employment so they could be weighted by industry employment to estimate national impacts.

7.1.1 End-User Benefits

The Internet survey provided most of the information used to estimate metrics related to systems administration benefits. Based on the survey results, RBAC is found to reduce the amount of time needed to perform several administrative activities, relative to alternative access control models. We also calculated benefits for employee downtime based on survey results. These estimates are discussed below.

However, although respondents also indicated that RBAC could generate organizational productivity, reduce upper management costs, and afford the security benefits, we had only sporadic information necessary to estimate these benefits. As a result these benefit categories are not included in our quantitative results and impact estimates.

Three realities hindered the collection of quantitative data on RBAC's impact on organizational productivity, upper management cost, and systems security and integrity:

- First, most enterprises have unique organizational structures and business models and practices, even among firms in

similar industries. Thus, drawing and developing comparisons across firms based on hypothetical scenarios regarding the impact an administrative tool may have on a firm's business practices is difficult. Impacts vary widely by firm, and most firms are unable to estimate impacts without any real world experience.

- Second, firms, and indeed individuals within firms, have different definitions of what constitutes a business event. For example, Internet survey respondents were able to evaluate the amount of time needed to terminate and assign user permissions for a given access control technology, but they may have been unable to evaluate systems security violations. A security violation for one firm may be when a user attempts to access information to which that user does not have access. For another firm, a security violation may occur when an unauthorized user accesses and affects a system's integrity.
- Finally, firms are hesitant to respond to questions that ask about sensitive information on their business operations.

For these reasons, we were not able to gather sufficient information concerning organizational productivity, upper management, and security benefits to develop defensible impact estimates. However, the case study in Section 5 does detail organizational productivity benefit that may be realized by using RBAC systems. In addition, several trade magazines have conducted annual reviews of information security managers, and key findings from these studies are discussed below.

7.1.2 RBAC Reduces Administrative Processing Time

Table 7-2 presents the amount of time required to perform four common activities using RBAC and non-RBAC models:

- assigning existing privileges to new users,
- changing existing users' privileges,
- establishing new privileges for existing users, and
- terminating privileges.

RBAC reduces the amount of time needed to assign privileges to new users by 5.5 minutes. RBAC reduces the time required to terminate a user's privileges by nearly 3 minutes. The time needed to alter a user's privileges is reduced by slightly more than 1 minute with RBAC.

Table 7-2. Average Task Time (Minutes) by Access Control System

	Assigning Existing Privileges to New Users	Changing Existing Users' Privileges	Establishing New Privileges for Existing Users	Terminating Privileges
RBAC systems	6.9	6.6	8.0	4.7
Non-RBAC systems	12.4	7.8	9.2	7.6
Difference	5.5	1.2	1.2	2.9

These four basic tasks are performed repeatedly every year and encompass a large percentage of an organization's total annual number of hours spent on systems administration. Table 7-3 presents the average number of times survey respondents conduct each of the four activities on an annual basis, both in absolute terms and per employee. The Internet survey respondents were with little exception large firms, each employing thousands of employees and maintaining vast information resources and networks. Consequently, it was common for one respondent to provide activities and time estimates for several different access control technologies.

Table 7-3. Number of Times Administrative Tasks Are Performed

Administrative Task	Average Number of Times per Year	Per Year, Per Employee
Assigning existing privileges to new users	1,802	1.30
Changing existing users' privileges	1,975	1.50
Establishing new privileges for existing users	1,000	1.06
Terminating privileges	452	0.22

It is important to distinguish between new users and new employees. New users may be new employees as well as current employees that are granted new permissions. Because many firms also maintain multiple access control systems and have many users with multiple user IDs the number of new users may significantly exceed the number of new employees hired annually. As such, the

per-employee estimate included in Table 7-3 should not be used to approximate employee turnover.

The per-employee average number of tasks performed allows us to estimate the administrative benefits a firm may accrue using RBAC when it is coupled with RBAC time-savings estimates and the average wage of employees performing the tasks. Using wage estimates provided by the Bureau Labor Statistics, this study estimates the loaded wage for systems administrators to be $51.62 per hour.[1]

The averages in Tables 7-2 and 7-3 underlie the benefits calculation portion of the economic model used to estimate the economic impact of RBAC. Based on this information, as shown in Table 7-4, an average firm with 100,000 employees could expect to save approximately $934,000 a year on systems administration using RBAC. Assigning existing privileges to new users accounts for over two-thirds of the administrative benefits.

Table 7-4. Systems Administration Benefit for a Typical Company with 100,000 Employees

Administrative Task	RBAC Time Savings per Task (minutes)	Average Number of Tasks per Year	Annual Total Benefit
Assigning existing privileges to new users	5.5	130,000	$615,138
Changing existing users' privileges	1.2	150,000	$154,860
Establishing new privileges for existing users	1.2	106,000	$109,434
Terminating privileges	2.9	22,000	$54,889
Total			$934,321

7.1.3 RBAC Increases Productivity

Section 4 hypothesized that RBAC had three potential productivity benefits: reduction in new employee downtime, enhanced

[1] According to the 2000 National Occupational Employment and Wage Estimates published by the Bureau of Labor Statistics, the mean wage for network and computer systems administrators is $25.81 per hour, or $53,685 annually. This estimate was multiplied by 2.0 to estimate the additional cost to the employer for employee benefits, such as employer-sponsored health and dental insurance and 401(k) contributions, as well as administrative and overhead costs.

organizational productivity, and reduced decision-making time for upper management. Information to estimate the reduction in new employee downtime was provided by telephone and Internet survey respondents, and this benefit component is included in the quantitative impact estimates. However, respondents were unable to provide quantitative data on RBAC's impact on organizational productivity or reduced decision-making time for upper management.

The length of downtime reported by survey respondents for new employees or current employees changing positions varied. Estimates ranged from 1 to 24 work hours, with most falling between 4 and 8 work hours. For current RBAC users and those in the process of implementing RBAC, the average employee downtime was 4.3 hours. Non-RBAC users experienced an average of 8.8 hours in downtime (see Table 7-5). This yields an average benefit of RBAC of 4.5 fewer hours of new employee downtime.[2]

Table 7-5. Reduction in New Employee Downtime (hours)

Metric	Non-RBAC System	RBAC System
Maximum downtime value	24.0	8.0
Minimum downtime value	0.5	0.5
Average downtime value	8.8	4.3

However, the term downtime is somewhat misleading. Conversations with IT professionals and managers revealed that employees are not totally unproductive when they do not have their permissions—they are simply less productive. Other activities, such as reading printed materials, attending meetings, attending orientation, introducing themselves to clients and coworkers, can be accomplished without access privileges. Some firms have temporary user IDs that new employees are assigned until the permanent ID is received. Knowledgeable professionals suggest that employees are about 80 to 90 percent productive during this

[2]The downtime savings estimate is not directly comparable to the RBAC systems administration benefits because the downtime estimate represents elapsed business hours from the time the new employee starts to the time he receives access. Changes in administrative time include paperwork and processing time needed to complete the task of actually assigning the permissions within the system. The difference between the two is the time the new employee's request sits in the queue waiting to be processed.

downtime. Therefore, we assume that new employees are about 85 percent as productive as they could otherwise be, given they are new to the position.

Table 7-6 shows the downtime reduction benefits of RBAC compared to non-RBAC systems. The difference of 4.5 hours, with a productivity loss of 15 percent yields a productivity loss of 0.67 hours. Using the average number of new employees per user in Table 7-3, a typical company with 100,000 employees would benefit approximately $3.4 million per year.

Table 7-6. Benefits from Reduced Downtime for a Typical Firm with 100,000 Employees

Metric	Non-RBAC System
Change in average employee downtime (RBAC vs. non-RBAC)	4.5 hrs
Productivity loss (15 percent)	0.67 hrs
Hourly rate	$39.46[a]
New users per employee	1.3
Annual benefits (100,000 employees)	$3,436,966

[a]According to the 2000 National Occupational Employment and Wage Estimates published by the Bureau of Labor Statistics, the mean wage for civilian white collar workers is $19.73 per hour, or $$41,038 annually. This estimate was multiplied by 2.0 to estimate the additional cost to the employer for employee benefits, such as employer-sponsored health and dental insurance and 401(k) contributions, as well as administrative and overhead costs.

7.1.4 RBAC Reduces the Severity and Frequency of Security Violations

When a security violation occurs, firms and organizations experience direct and indirect costs. Depending on the industry and the nature of the security violation, the impacts are potentially large. In a 2000 *Information Security* magazine survey, nearly 2,000 information security managers were asked if they had experienced a security violation within the past year from employee access abuse, unauthorized access by outsiders, access abuse from nonemployee authorized users, or the leakage of proprietary information. According to *Information Security*, 58 percent of the respondents reported violations due to employee access abuse, 42 percent due to unauthorized access by outsiders, 14 percent due to access abuse by nonemployee authorized users, and 24 percent due to the leakage of proprietary information (Briney, 2000).

Not only are security violations occurring with frequency, they are costly. Table 7-7 presents average cost per violation from the Computer Security Institute (2001) located in San Francisco. Theft of proprietary information and financial fraud are typically the most costly forms of security violation.

Table 7-7. Average Cost per Security Violation 1999 – 2001 ($thousands)

Type of Violation	1999	2000	2001
Theft of proprietary information	1,848	3,033	4,448
Sabotage	164	970	199
Telecom	77	66	55
System penetration	103	245	454
Insider abuse of net access	94	307	357
Financial fraud	1,471	1,647	4,421
Denial of service	116	109	122
Virus contamination	45	180	244
Unauthorized access to information by insider	143	1,125	276
Telecom fraud	27	212	502
Active wiretapping	20	5,000	0
Laptop theft	87	59	62

Source: Computer Security Institute. 2001. "2001 CSI/FBI Computer Crime and Security Survey." *Computer Security Issues and Trends* VII(1):Spring.

With the increasing use of e-commerce, the potential for security violations will increase, as may the cost. RBAC systems are designed to mitigate the possibility of these violations occurring, although this study was unable to predict the extent to which they will do so.

7.1.5 End-User Customization and Installation Costs

Customization and installation costs for end users are based primarily on the case study. As described in Section 5.4, the customization and implementation cost per user less software costs is estimated to be approximately $78.36.

Information from the survey respondents that had implemented or were implementing RBAC at the time of the telephone and Internet surveys corroborate the detailed estimates from the case study.

However, information from the surveys was less detailed and it was not always clear what activities were being included in their cost estimates.

A summary of the findings from the Internet study are presented in Table 7-8. The details provided by respondents concerning their implementation and customization costs varied. Some companies fully disclosed the processes they used, whereas others provided only general estimates for a few of cost categories.

Table 7-8. End-User Customization Costs, Evidence from Internet Survey

Metric	Internet Study Value	Case Study Value
Average total amount of time needed to fully implement RBAC	12 months	15 months
Average time required to migrate user base to RBAC	6 months	6 months[a]
Average customization and implementation costs for purchased system, consulting fees	$100,000	$44,000[b]
Hardware costs	$17,000	$20,000
Number or full-time employees required	1 to 4	3

[a]Excludes staggered rollout of extranet users and internal users.

[b]Sum of maintenance and support agreement and consulting fees less software costs.

Most of the survey respondents stated that the process of rolling out RBAC took or would take about 1 year, and that the process of bringing users online in the RBAC system takes approximately 6 months. They also indicated that hardware purchases were made to facilitate migration and implementation, and that they hired consultants, either the software vendor or a third-party organization, to assist in implementation. The expense attributable to consulting fees averaged approximately $100,000.

We use the detailed cost per user estimates developed from the case study as the basis for typical firm cost in the empirical analysis for several reasons:

- The case study results give a more complete picture of an average firm's implementation expenses. Many survey respondents left out one or more cost categories. It was possible to assemble a general impression of costs using their responses, but no one response yielded enough information to completely calculate costs per user for their firms.

- Because of the number and depth of the interviews conducted with the case study participant, the cost estimate from the case study does provide a complete portrayal of adoption activities.
- Finally, as Table 7-8 indicates, the results from the case study closely match those from the Internet survey and end-user interviews.

Included in the end-user adoption costs are all customization and implementation costs with the exception of software expenditures. Software expenditures are treated as a transfer payment from end users to software developers. The R&D costs of software developers are included as a separate cost category and are discussed in the following subsection.

7.2 R&D COSTS ASSOCIATED WITH DEVELOPING RBAC PRODUCTS AND SERVICES

Organizations conducting research into RBAC and RBAC-enabled products and services are for the most part software vendors producing commercial packages. However, some software end users are also developing or have developed RBAC systems in-house.

7.2.1 Software Vendors' R&D Costs

The average R&D cost for software developers to integrate RBAC functionality into their products is estimated to be approximately $550,000. This average R&D budget was developed from the responses software developers provided during the telephone interviews and a limited number of Internet survey responses.

The highest R&D budget reported was $1 million, and the lowest $100,000. A company that has incorporated the most advanced model of RBAC into its products provided the $1 million estimate. The $100,000 estimate reflects a company that incorporated lower levels of RBAC functionality. The remaining companies were distributed fairly evenly between these upper and lower bounds. As a result, the midpoint of the budget range, $550,000, was selected for typical R&D costs for software developers.

At the time this study was completed, approximately 26 software companies were known to market RBAC and RBAC-enabled products. Other companies are likely in the process of developing

RBAC-compatible products, but much of this information is proprietary. End users are showing significant interest in RBAC; therefore, we anticipate that the number of companies offering RBAC and RBAC-enabled products will increase over the next few years.

It is not known with certainty when these companies first began to integrate RBAC into their products, but we do know that some of their RBAC-enabled products were first on the market in 1997 and 1998. Most software companies indicated that integrating RBAC functionality took up to 1 year. Therefore, our analysis models R&D costs beginning in 1996 and with an average of five products begin developed each year between 1996 and 2000.[3] Based on interviews, software developers spent on average $550,000 developing their RBAC-enabled products. This yields industry expenditures of approximately $2.75 million per year. To account for enhancement to existing products and firms that will be marketing new RBAC products in the future, this R&D rate is extrapolated through our time horizon of 2005.

7.2.2 In-house End-User Development Costs

Telephone interviews with end users indicated that few companies have developed RBAC products in-house because of the amount of labor hours and level of expertise required. Furthermore, it is unclear what percentage of end users may be in the process of or considering developing an system in-house in the future rather than purchase a commercially available solution. For this quantitative analysis, we assumed the five large companies per year would be developing in-house systems at a cost of $550,000 per system.

End users that do pursue an in-house strategy will do so because their organizational structure, size, and their user structure would warrant devoting the resources to it. For example, the three respondents to Internet survey and end-user telephone interviews that developed some type of RBAC system in-house noted that their organization each employed more than 100,000 people. The one exception to the trend of in-house developers is one small security company whose line of business warranted early adoption of

[3]Five firms per year is based on 26 companies that are known to presently market RBAC products that were developed over the 5 year period from 1996 through 2000.

RBAC. The sum of this company's employee and user base was 150. The total cost of development for this company was $68,066 over the course of a 1-year period, or $453.77 per user (see Table 7-9).

Table 7-9. One End-User's In-House RBAC Development Costs

Metric	Cost
Design and development cost	$25,000
Implementation cost[a]	$28,066
Hardware costs	$15,000
Total cost	$68,066
Cost per user	$453.77

[a]This respondent indicated that its implementation expense was 6 months at 60 labor hours a month. Using the standard $77.96 loaded wage rate for systems administrators used through this report, the total implementation cost is estimated to be $28,066.

7.3 CURRENT AND PROJECTED DIFFUSION OF RBAC

In general RBAC is still in the early stages of adoption. Most commercial products have only been available for a year or two and companies are just beginning to realize the potential savings RBAC presents.

Companies that responded to our survey varied with respect to their current stage of RBAC development. Respondents were asked if they were considering adopting an RBAC system, were in the process of designing one, were in the process of implementing one, currently operating one, or had no plans to change access control systems. Table 7-10 gives the share of respondents in each of these categories. The most common response was that their company was considering adopting an RBAC system. It should be noted that survey response bias may have an upward bias on the implied current penetration of RBAC. Firms that have no interest or have not heard of RBAC are less likely to complete the survey.

Companies that had systems in place or were in the process of implementation were all in the financial services and health case sectors. Other industries considering adoption were information technology, transportation, telecommunications, and electric utility.

Table 7-10. Respondents' Current Stage of RBAC Development

Status	Percentage
Considering adopting an RBAC system	42%
In the process of designing an RBAC system	8%
Currently implementing an RBAC system	12%
Have RBAC system in operation	12%
Have no plans to adopt an RBAC system	27%
Total	100%

Software developers believed that the greatest growth in the adoption of RBAC will continue to be in the health care, financial services and insurance, and information industries. These three industries currently conduct the majority of their information transactions electronically, and significant inefficiencies exist in current access control management.

Software developers also indicated that most industries, to some degree, would implement some form of RBAC-enabled system by 2005. They thought that substantial growth will be seen in the information sector, which includes technology and telecommunications. However, penetration in this industry will be slower than in the aforementioned three because the regulatory and security drivers are not as strong for the majority of constituent companies. Data gathered during an exercise with the Network Applications Consortium (NAC), an association of large software-systems end users, confirmed these trends. Software developer and NAC responses were averaged to estimate the RBAC market penetration rates presented in Table 7-11.

As described above, industry experts are in basic agreement about which sectors will be most active in adopting RBAC systems. However, there was less consensus in the realized rate of penetration by 2005. Because of this uncertainty, three diffusion scenarios are used to present the empirical estimates. These scenarios represent low, medium, and high rates of projected penetration. These scenarios are presented in Table 7-11 by industry sector. Industry penetration is expressed as the percentage

Table 7-11. RBAC Penetration Rates by Industry, 2005

	Information[a]	Finance and Insurance	Health Care and Social Assistance	Government[b]	Educational, Professional, Scientific, and Technical Services	Manufacturing	Utilities	Transportation and Warehousing
Number of Firms (500+ Employees)	969	1,640	3,414	1	3,089	4,838	232	1,110
Employment in Firms (500+ Employees)	2,238,831	3,889,704	7,304,840	2,425,898	3,271,963	9,931,342	578,717	1,955,724
Market Penetration Rates by 2005								
Low	20	35	40	5	10	5	15	15
Medium	30	45	50	10	15	10	25	25
High	40	55	60	15	20	15	35	30
Number of Employees Managed Using RBAC by 2005								
Low	447,766	1,361,396	2,921,936	121,295	327,196	496,567	86,808	293,359
Medium	671,649	1,750,367	3,652,420	242,590	490,794	993,134	144,679	488,931
High	895,532	2,139,337	4,382,904	363,885	654,393	1,489,701	202,551	586,717

[a]Information includes telecommunications.

[b]This analysis assumes that by 2005 only departments and agencies within the federal government will have adopted RBAC.

of employees in companies with employment greater than 500 that will be managed by RBAC systems by the end of 2005. Note that the relative adoption trends across industry sectors are maintained in each of the three scenarios.

7.4 NIST'S IMPACT ON THE DEVELOPMENT AND ADOPTION OF RBAC

This section presents software developers' understanding and valuation of NIST's contributions to the development of RBAC. Based on the telephone interviews, almost all software developers indicated that NIST's research and sponsorship have accelerated the RBAC development process. In addition, they indicated that NIST's activities have lowered the cost of integrating RBAC functionality into their products; however, they said that the cost impact was secondary.

All the developers interviewed were familiar with NIST's articles in the professional literature, and many have attended at least one workshop or conference that was either sponsored by NIST or contained a presentation or information by NIST on the subject. However, software developers also indicated that they believe NIST has had no measurable impact on reducing end-user customization and implementation costs and enhancing the overall quality of RBAC products.

7.4.1 Accelerated Adoption and Availability

Developers interviewed agreed that without NIST's contributions and sponsorship RBAC would not be as evolved as it currently is.

Most developers believe that NIST's research accelerated the rate of RBAC adoption by 1 year and consequently the availability of RBAC products by 1 year. In other words, the market introduction for the average software product was moved forward 1 year because of NIST's research and RBAC awareness activities. One large software developer stated:

> The NIST prototype … demonstrated the practicability of role-based access control, serving as a reference point and galvanizing customer interest. This helped to validate the importance of RBAC with respect to other possible approaches. It also clarified which potential RBAC features were central and most useful in our particular environment.

A second developer stated that without NIST's research the state of RBAC development would not have been able to reach its current level of development until approximately 2004 or perhaps even 2005, but this developer was the only one of the eight to provide such a large acceleration estimate. The remaining developers were more conservative, stating that the time horizon was shifted forward by an average of one year. All developers interviewed agreed that without NIST's contributions and sponsorship RBAC would not be as evolved as it currently is.

7.4.2 Reduced R&D Expenditures

Most software developers interviewed indicated that NIST's contributions have lowered the R&D costs on integrating RBAC into their software products. However, many had difficulty quantifying the magnitude of the impact. Based on respondents that did provide quantitative changes in labor costs, we estimate that NIST's research reduced developers' R&D expenditures by an average of 8.2 percent.

NIST's work not only made developers aware of alternative access models, but it also provided a significant amount of research and prototype code. It may take some time before more developers include NIST's work on constraints and role hierarchies in their products, although a small subset of developers has already done so. But even the developers implementing lower levels of RBAC credited NIST with lowering R&D costs. Developers agree that benchmarks provided by NIST's research have had the benefit of reducing front-end R&D costs. Savings were expressed in terms of labor hours and computing resources.

The more complex an RBAC software product's features are, the more its software developer leverages NIST's research. Developers that included only the most basic RBAC functionality in their products do not directly leverage NIST's research into constraints and hierarchies. Therefore, the impact NIST's research has had on their design and development costs would not be as significant as for those developers that do incorporate those advanced capabilities. It is possible that as more advanced RBAC functionalities are included in more commercial products NIST's incremental impact will increase.

One software developer noted that, although his product does not incorporate constraints or role hierarchies as defined by NIST, the NIST RBAC model underlies his principal product offering. He stated that without NIST's research, his company never would have "gotten off the ground; the research and development would have been too costly." Using the open platform provided by NIST, the company was able to first replicate the NIST model and then augment and tailor it to meet the specifications required in target industries.

A second software developer stated:

> The NIST implementation was a groundbreaking and significant contribution to software technology. But its value didn't come from being a "model" that could simply be imitated.
>
> As we see it, the greatest value of the NIST implementation was in animating a discussion throughout the industry, and we were able to benefit from that discussion, as were many others. This is probably one of the best examples of how an organization like NIST can help the private sector. The existence of a widely visible prototype advanced the concrete understanding of corporate IT architects so significantly that we were able to get unusually good early feedback validating and influencing our design choices. Getting educated feedback early undoubtedly saved us a significant amount of money.

A second developer said that NIST's research saved his company 640 hours in development time by speeding up the development of his product's RBAC functionality. He used NIST's research to formulate the fundamentals of this particular functionality and to develop design specifications. Given that the average R&D budget used to develop RBAC functionality is $550,000, and that the average loaded hourly wage of people conducting this research is $70.60, we estimate that the developer avoided $45,184 in labor

costs, or 8.2 percent of their R&D budget.[1] This percentage reduction in R&D costs is used in the quantitative analysis as the typical cost savings experienced by software developers.

7.4.3 Reduced End User Customization and Implementation Costs

Developers indicate that NIST's activities have not affected the private cost of customizing and implementing RBAC and RBAC-enabled products. End users customize software to meet their data and applications needs and to configure it to correspond to their system's structure. End users indicated that accelerating the rate of the availability of RBAC products does not make the process of introducing them in the workplace any less time consuming or costly. The customization and implementation processes that end users experience would be no different under the without-NIST scenario than the with-NIST scenario. Likewise, the costs that end users incur in completing these tasks would be the same.

7.4.4 RBAC Product Enhancement

Although interviewees did agree that NIST publications and patents facilitated the R&D process, estimating the overall impact of NIST's research on the quality of RBAC-enabled products is difficult. None of the software developers interviewed felt that NIST's activities lead to better, higher quality, RBAC software products.[2] One software developer stated:

> We had arrived independently at many of the concepts that appeared in the NIST work, but NIST's contribution was critical in establishing a taxonomy and a shared vocabulary for us, our customers and the industry as a whole.

Developers note that it is unlikely that any one company would incorporate 100 percent of a NIST model. Rather they would supplement their own work with NIST's, using NIST's research to

[1] According to the 2000 National Occupational Employment and Wage Estimates published by the Bureau of Labor Statistics, the mean wage for computer and information research scientists is $35.30 per hour, or $73,424 annually. This estimate was multiplied by 2.0 to estimate the additional cost to the employer for employee benefits, such as employer-sponsored health and dental insurance and 401(k) contributions, as well as administrative and overhead costs.

[2] Although, at noted earlier, by NIST accelerating the introduction of RBAC, the quality of access control products in general has been improved.

form a portion of the foundation of their products or as an example of future product capabilities. One developer stated:

> There are pieces in our model that don't exist in the NIST model—for example, the notion of "scope," which is very fundamental to solving the kinds of issues that present themselves in a highly distributed infrastructure such as Windows 2000. There are also things in the NIST model which we concluded were of limited application in the type of infrastructure we animate.

A second developer stated that software developers might use, -on average, 30 to 40 percent of a NIST model. This is in keeping with earlier findings that several components of NIST's models have not been incorporated into commercial product offerings. They deem NIST's research helpful, but as in the words of one developer, products "need to walk before they can run."

Software developers foresee the inclusion of advanced nesting, constraints, and hierarchies in future products. Their comments suggest that NIST research in these areas will increase product offerings and reduce the cost of these traits' inclusion. At present the NIST prototype code is considered too complicated. But as RBAC technologies and applications progress and more companies enter the market, software developers agree that the likelihood that more advanced components of NIST's research will be included in products will increase.

8 Measures of Economic Return

To estimate the measures of economic return from the NIST/ITL RBAC project, we first developed a baseline time series of the benefits and costs of RBAC. We then shifted this baseline time series that includes NIST's contributions to reflect a counterfactual world without NIST's impact on the development and adoption of RBAC. The value of NIST's contributions is calculated as the change in the net benefits of RBAC with and without the NIST/ITL RBAC project. As presented in Section 6, the two NIST impact categories quantified through the data collection activities are the reduction in R&D expenditures and the acceleration of the development and adoption of RBAC systems.

8.1 BASELINE TIME SERIES OF THE BENEFITS AND COSTS OF RBAC

The baseline time series is the observed world that included NIST's contributions. Most industry experts agreed that significant penetration of existing products would be achieved by 2005. Thus, we model baseline benefits and costs associated with RBAC through 2006, one year after the penetration projections provided by industry.

The fundamental components of benefits and costs associated with RBAC are described in Section 3. Eq. (3.2) shows the calculation of the time series net benefits (NB_t). This equation is repeated below for convenience.

$$NB_t = R\&Dsd*Nsd_t + R\&Dih*Nih_t + \Sigma\,[(OB_{it}+IC_{it})*Emp_{it}]$$

8.1.1 Benefit and Cost Components

Table 8-1 summarizes the key benefit and cost estimates described in Section 6 and links them to the variables in the net benefit equation.

Table 8-1. Key Benefit and Cost Estimates

Description	Variable	Value
R&D costs to integrate RBAC into software developers product	R&Dsd	$550,000 per software company
Number of software developments per year	Nsd_t	Five software companies per year
R&D costs to develop in-house RBAC software	R&Dih	$550,000 per in-house development
Number of in-house developments per year	Nih_t	Five in-house developments per year
End-user annual operational benefits per employee	Ob_{it}	$43.57 per employee
End-user customization and implementation costs per employee	IC_{it}	$78.36 per employee
Number of employees managed by RBAC systems at time t	Emp_{it}	Three diffusion scenarios

R&D Expenditures

In the baseline time series, R&D expenditures begin in 1996, 1 year prior to the introduction of the first major RBAC products. Constant annual costs of $5,500,000 continue through the projection year of 2006.[1]

End-User Benefits

The annual operating benefits of RBAC are $43.57 per employee. This is held constant across industries. Employees first begin to be managed by RBAC systems in 2001; hence benefits are first realized in this year. The growth of employees managed using RBAC systems is assumed to follow an S-shaped diffusion.

[1] Annual R&D costs are the sum of five software developers and five in-house developers each at $550,000. A constant level of annual expenditures is used because little information was available on the timing of the product development for the 26 currently available RBAC products or for R&D expenditures associated with in-house development.

End User Costs

Average end-user customization and implementation costs are estimated to be $78.36 per employee. These costs per employee are incurred 1 year prior to the realization of benefits. Thus, end-user customization and implementation costs begin in 2000. The time series of end-user costs follow the same diffusion patters described below but are lagged 1 year prior to the realization of benefits.

8.1.2 Diffusion of RBAC by Employee

Because the future rate of penetration is uncertain, three different diffusion scenarios are used, reflecting a low, medium, and high penetration scenario. Table 8-2 repeats the three penetration scenarios by industry presented in Table 6-11. The percentage penetration in Table 8-2 gives the level of market penetration as of the last year of the analysis, 2006.

Table 8-2. Industry Employment and Baseline Diffusion Scenarios

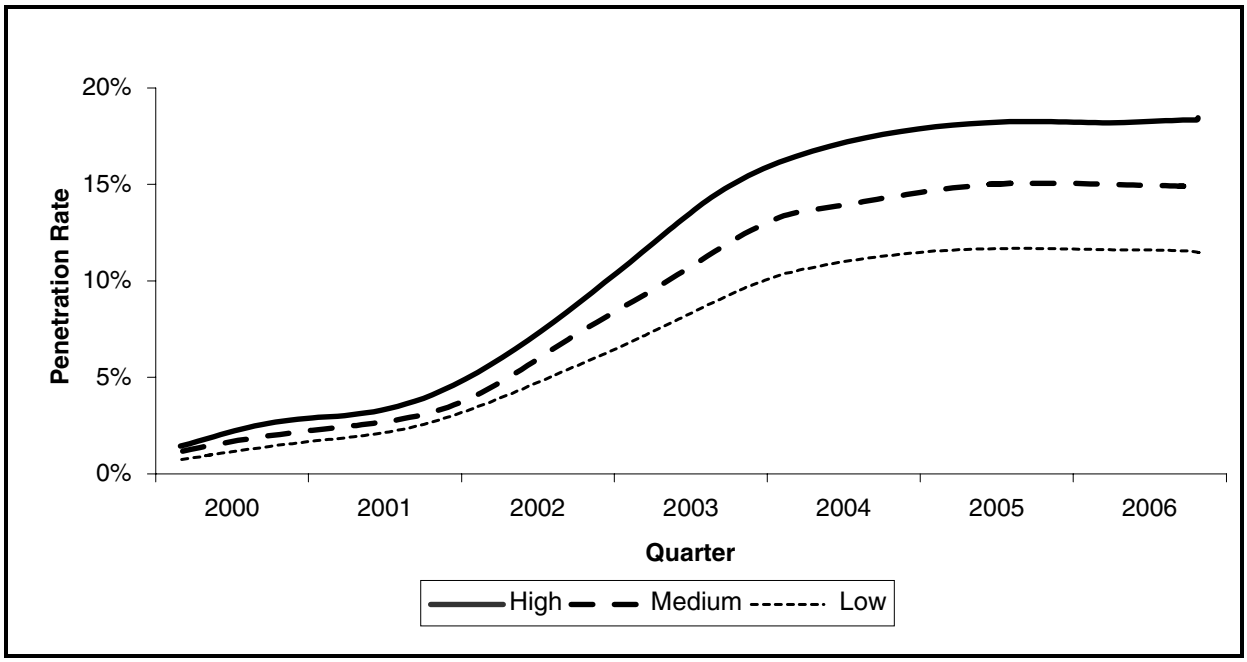
Industry	Low	Medium	High	Employment[a]
Information	20	30	40	2,238,831
Finance and insurance	35	45	55	3,889,704
Health care and social assistance	40	50	60	7,304,840
Educational, professional, scientific, and technical services	10	15	20	3,271,963
Manufacturing	5	10	15	9,931,342
Utilities	15	25	35	578,717
Transportation and warehousing	15	25	30	1,955,724
Total				29,171,121

[a]Industry employment for companies with more than 500 employees.

The total employment figures in Table 8-2 include employment of firms having more than 500 employees. This size cutoff was chosen based on conversations with industry experts and reflects a typical critical mass where RBAC is more likely to be adopted. We summed the total employment across industries to obtain an estimate of the total employment size to use for the analysis.

Given the final penetration rate with a particular scenario, we fit a logistic S-shaped curve to the data for each industry and then aggregated the curves with respect to time. Figure 8-1 shows the aggregate curves for the three penetration rate scenarios where each curve is an employee-weighted penetration curve that aggregates industry penetration.

Figure 8-1. Aggregate Penetration Rates for Low, Medium, and High Rate Scenarios



8.1.3 Time Series of RBAC Benefits and Costs

Table 8-3 presents the time series of RBAC benefits and costs for the medium penetration scenario. R&D expenditures and end-user costs are shown as negative benefits. Net benefits begin negative reflecting early R&D expenditures and then become positive in 2002 as RBAC penetration increases.

8.2 NIST'S IMPACT ON THE BENEFITS AND COSTS OF RBAC

NIST's contributions to the development and adoption of RBAC affect the time series of benefits and costs shown in Table 8-3 by

Table 8-3. Baseline RBAC Benefits and Costs ($millions)[a]

Year	R&D Expenditures: Software Developers and In-House Development[b]	End-Users' Customization and Implementation Costs[b]	End-Users' Operation Benefits	Net Benefits of RBAC
	$R\&Dsd*Nsd_t + R\&Dih*Nih_t$	$\sum_i IC_{it}* Emp_{it}$	$\sum_i Ob_{it}* Emp_{it}$	NB_t
1992[c]	—	—	—	—
1993	—	—	—	—
1994	—	—	—	—
1995	—	—	—	—
1996	–5.05	—	—	–5.05
1997	–5.05	—	—	–5.05
1998	–5.05	—	—	–5.05
1999	–5.05	—	—	–5.05
2000	–5.05	–13.03	—	–18.08
2001	–5.05	–19.72	24.41	–0.36
2002	–5.05	–36.48	61.37	19.84
2003	–5.05	–64.40	129.71	60.26
2004	–5.05	–38.24	250.37	207.08
2005	–5.05	–8.45	322.01	308.51
2006	—	—	337.85	337.85
NPV (2000)	–53.23	–161.67	885.98	671.08

[a]All numbers have been adjusted to 2000 dollars.
[b]Expenditures are shown as negative benefits.
[c]Time series begins in 1992 because this is the first year of NIST expenditures.

- ➤ lowering R&D costs for software developers and in-house developers and
- ➤ accelerating the RBAC development and adoption process.

8.2.1 NIST's Impact

Table 8-4 summarizes the key change metrics needed to estimate the economic impact of the NIST/ITL RBAC project in terms of the variables in the net benefit change (ΔNB_t) equation presented in Section 4 (Eq. [4.2]). This equation is repeated below for convenience.

$$\Delta NB_t = \Delta R\&Dsd*\Delta Nsd_t + \Delta R\&Dih*\Delta Nih_t + \sum[(OB_{it}+IC_{it})*\Delta Emp_{it}]$$

Table 8-4. Key Metrics for NIST's Impact

Variable	Value	Comment
ΔR&Dsd	$31,900 per software company	5.8 percent reduction in R&D costs
ΔNsd_t	1 year	R&D activities are accelerated by 1 year for all software companies
ΔR&Dih	$31,900 per in-house development	5.8 percent reduction in R&D costs
ΔNih_t	1 year	R&D activities are accelerated by 1 year for all in-house developments
ΔEmp_{it}	1 year	Diffusion is accelerated by 1 year

Without NIST's contributions software developers and in-house developers would not have been initiated until 1997 (1-year delay) and R&D expenditures would have been 5.8 percent greater.

The 1-year delay would also have delayed the realization of benefits (and costs) for end users. However, NIST's influence does not alter the shape of the end-user diffusion curve; it just creates a parallel shift backward of 1 year.

8.2.2 Time Series of Counterfactual Benefits and Costs

Table 8-5 shows the time series of benefits and costs for the baseline, counterfactual, and the difference, which is the change in net benefits attributable to NIST. The time series is for the medium penetration scenario. The net present value of NIST's impact on the benefits of RBAC is $295 under the medium penetration scenario.

8.3 CALCULATING MEASURES OF ECONOMIC RETURN

This change in net benefits attributable to NIST is compared to NIST's expenditures to estimate measures of economic return to the NIST/ITL RBAC project. The time series of NIST expenditures for the medium penetration scenario is shown in Table 8-6. The NPV of NIST/ITL expenditures on the RBAC projects described in Section 2.6 are approximately $2.7 million.

Table 8-5. Time Series of Industry Net Benefits With and Without NIST's Contributions ($millions)[a]

Year	Baseline (with NIST)	Counterfactual (without NIST)	Total Change in Net Benefits (ΔNB_t)
1992	—	—	—
1993	—	—	—
1994	—	—	—
1995	—	—	—
1996	–5.05	—	–5.05
1997	–5.05	–5.50	0.45
1998	–5.05	–5.50	0.45
1999	–5.05	–5.50	0.45
2000	–18.08	–5.50	–12.58
2001	–0.36	–16.90	16.54
2002	19.84	–0.33	20.17
2003	60.26	18.54	41.72
2004	207.08	56.32	150.76
2005	308.51	193.53	114.97
2006	337.85	288.33	49.52
NPV (2000)	671.08	376.31	294.77

[a]All numbers have been adjusted to 2000 dollars.

We used NIST's expenditures and their related impact on the net benefits of RBAC to calculate a net present value (NPV), benefit-cost ratio, and an internal rate of return (IRR). The NPV of NIST's expenditures is the difference between the NPV of the change in the net benefits to RBAC less the NPV of NIST's expenditures. The benefit-cost ratio provides the NPV measure of the benefits of the project relative to the NPV costs of the project. The IRR is a measure of what the interest rate would need to be to make the initial costs of the project greater than the long-run return from the project. These measures of economic return are described in detail in Section 4.

The three measures of economic return are presented in Table 8-7. The measures are shown for the three penetration scenarios. The NPV of NIST's impact under the medium penetration scenario is $292 million. The benefit-cost ratio ranges from 69 to 158, and the IRR ranges from 39 to 90 percent.

Table 8-6. Time Series of Net Benefits due to NIST's Contributions and NIST Expenditures ($millions)[a]

Year	Total Change in Net Benefits	NIST Expenditures
1992	0.00	0.06
1993	0.00	0.06
1994	0.00	0.19
1995	0.00	0.47
1996	–5.05	0.45
1997	0.45	0.39
1998	0.45	0.34
1999	0.45	0.04
2000	–12.58	0.04
2001	16.54	0.04
2002	20.17	0.00
2003	41.72	0.00
2004	150.76	0.00
2005	114.97	0.00
2006	49.52	0.00
NPV (2000)	294.77	2.70

[a]All numbers have been adjusted to 2000 dollars.

Table 8-7. Measures of Economic Return to the NIST/ITL RBAC Project ($millions)[a]

	High	Medium	Low
a. NPV change in net benefits	427.42	294.77	185.71
b. NPV NIST expenditure	2.70	2.70	2.70
NPV of the NIST/ITL RBAC project (a – b)	425	292	183
Benefit-cost ratio	158	109	69
Internal rate of return	90%	62%	39%

[a]All numbers have been adjusted to 2000 dollars.

References

Barkley, John F. 1995. "Application Engineering in Health Care." Second Annual CHIN Summit 1995.

Barkley, John F. and Anthony V. Cincotta. 1998. "Managing Role/Permission Relationships Using Object Access Types." Third ACM Workshop on Role-Based Access Control.

Barkley, John F., Anthony V. Cincotta, David F. Ferraiolo, Serban Gavrila, and D. Richard Kuhn. 1997. "Role Based Access Control for the World Wide Web." 20th National Computer Security Conference.

Briney, Andy. 2000. "Security Focused." *Information Security* September:40-68.

Byrnes, Christian, Vice-President: Services and Systems Management, The META Group. June 13, 1997. "Security Administration Grows Up." An analyst report produced for Tivoli, an IBM company.

Computer Security Institute. 2001. "2001 CSI/FBI Computer Crime and Security Survey." *Computer Security Issues and Trends* 7(1).

Ferraiolo, David F., and D. Richard Kuhn. 1992. "Role Based Access Control." 15th National Computer Security Conference.

Ferraiolo, D.F., D.M. Gilbert, and N. Lynch. 1992. *Assessing Federal and Commercial Information Security Needs*. NISTIR 4976. Gaithersburg, MD: National Institute of Standards and Technology.

Ferraiolo, D.F., J.A. Cugini, and R. Kuhn. 1995. "Role Based Access Control: Features and Motivations." *Proc. Eleventh Annual Computer Security Applications Conference*.

Ferraiolo, David F., and John F. Barkley. 1997. "Specifying and Managing Role-Based Access Control within a Corporate Intranet."

Ferraiolo, David F., John F. Barkley, and D. Richard Kuhn. 1999. "A Role Based Access Control Model and Reference Implementation within a Corporate Intranet." ACM Transactions on Information Systems Security 1(2).

Ferraiolo, David F., Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. 2001. "Proposed NIST Standard for Role-Based Access Control." ACM-Transactions, p. 17-47.

Gavrila, Serban, and John F. Barkley. 1998. "Formal Specification for Role Based Access Control Models and Access Control Lists." Third ACM Workshop on Role-Based Access Control.

Geroski, P.A. 2000. "Models of Technology Diffusion." *Research Policy* 29:603-655.

Health Care Financing Administration (HCFA). 2001. "General Questions." <http://www.hcfa.gov/extpart/faqs/faq-genqt.htm>. As obtained on June 13, 2001.

Hilchenbach, Burkhard. 1997. "Observations on the Real-World Implementation of Role-Based Access Control." 20th NISSC Proceedings. Baltimore, MD.

Infosecurity Magazine. July 1999. <http://www.infosecuritymag.com>.

Jaffe, A.B. December 1996. *Economic Impact Analysis of Research Spillovers: Implications for the Advanced Technology Program*. NIST GCR 97-708. Prepared for the U.S. Department of Commerce, National Institute of Standards and Technology, Advanced Technology Program.

Joshi, James, Arif Ghafoor, Walid G. Aref, and Eugene H. Spafford. 2001a. "Digital Government Security Infrastructure Design Challenges." *Computer* February:66-72.

Joshi, James, Walid G. Aref, Arif Ghafoor, and Eugene H. Spafford. 2001b. "Security Models for Web-Based Applications." *Communications of the ACM* 44(2):38-44.

Kuhn, D. Richard. 1997. "Mutual Exclusion of Roles as Means of Implementing Separation of Duty in Role-Based Access Control Systems." Second ACM Workshop on Role-Based Access Control.

Ledig, Robert. 2000. "Gramm-Leach-Bliley Act Financial Privacy Provisions: The Federal Government Imposes Broad Requirements to Address Consumer Privacy Concerns." Fried, Frank, Harris, Shriver & Jacobson. <http://www.ffhsj.com/bancmail/bmarts/ecdp_art.htm>. As obtained on June 14, 2001.

Mahajan, V., and R.A. Peterson. 1985. "Models for Innovation Diffusion." Sage University Paper Series on Quantitative Applications in the Social Sciences, 07-048. Beverly Hills and London: Sage Publications.

Martin, S.A., D.L. Winfield, A.E. Kenyon, J.R. Farris, M.V. Bala, and T.H. Bingham. 1998. "A Framework for Estimating the National Economic Benefits of ATP Funding of Medical Technologies—Preliminary Applications to Tissue Engineering Projects Funded from 1990 to 1996." Prepared for the National Institute of Standards and Technology. RTP, NC: RTI.

Sandhu, R. 1998. "Role-Based Access Control." *Advances in Computers* 46:237-286.

Sandhu, R., and P. Samarati. 1994. "Access Control Principles and Practice." *IEEE Communications* 32(9).

Sandhu, R., E. Covne, H. Feinstein, and C. Youman. 1997. "Role-Based Access Control Models." *IEEE Computer* 29(2):38-47.

Scott, John T. 1999. "The Service Sector's Acquisition and Development of Information Technology: Infrastructure and Productivity." *Journal of Technology Transfer* 24:37-54.

SETA Corporation. 1996. "A Marketing Survey of Civil Federal Government Organizations to Determine the Need for RBAC Security Product." Prepared for the National Institute of Standards and Technology.

Stiglitz, J.E. 1988. *Economics of the Public Sector*. New York: W.W. Norton & Company.

Tassey, Gregory. 1997. *The Economics of R&D Policy*. Westport, CT: Quorum Books.

U.S. General Accounting Office (GAO). July 2001. "Information Security: Weak Controls Place Interior's Financial and Other Data at Risk." Report to the Secretary of the Interior. GAO-01-615.

Appendix A: Questionnaire for RBAC Technology Developers

Questionnaire for RBAC Technology Developers

Introduction

On behalf of the National Institute of Standards and Technology (NIST), Research Triangle Institute (RTI) is investigating the benefits and costs of using Role-Based Access Control (RBAC) as an alternative to existing access control techniques. Specific issues of interest are

- the effect of NIST's involvement on the development of RBAC and commercial products incorporating RBAC,
- a comparison of the costs and benefits to end users of RBAC with other access control technologies, and
- the effect of NIST's involvement on the diffusion of RBAC.

Our study would benefit a great deal from your input. Please read and consider the enclosed questions as they relate to your company's products. We encourage you to collaborate with your colleagues when answering these questions, because several questions span a variety of aspects of the product design and development process.

Any information you provide will remain strictly confidential. In the published results of this study, information that you provide that is specific to your organization will not be presented explicitly and will not be attributed to your organization without your permission. Your name will not be shown. However, your organization's name will be acknowledged with appreciation in a list of survey participants.

You may complete the questionnaire online at https://public.rti.org/rbac/. All information transferred electronically will be encrypted. Alternatively, you can e-mail or fax your responses to us at bkropp@rti.org or (919) 541-6683. At any time, if you have any questions, please feel free to contact either Brian Kropp at (919) 485-5584 or Mike Gallaher at (919) 541-5935. Thank you for your input to our study.

1. Contact and Company Information

Contact Name: _____

Company Name: _____

Mailing Address: _____

Title: _____

Phone Number: _____

E-mail: _____

2. Market Penetration of RBAC

2.1 Please list and describe your company's software products and systems that embody RBAC technology. In particular, we are interested in additional or linked ACL functionalities (other than RBAC) incorporated into your products.

Product Name	Brief Description

2.2 Please describe how your RBAC technology product is used by firms or organizations to control and manage access to information and system resources?

2.3 Please list the major industries that use your product in Table 2-1 and, for each industry, indicate

- what competing technologies exist in these industries and
- the percentage of firms that are currently using an RBAC system in each industry.

Table 2-1. Industry Sectors Using Your Product

Industry	Competing Technologies	Current Percentage of Firms Using Role-Based Access Control
Example: Banking	***Identity-Based ACL***	***5%***

2.4 We are also interested in the penetration/adoption rate of RBAC into the near future. In Table 2-2, for the years listed, please estimate the percentage of firms that will be using an RBAC or RBAC-based product. Please provide separate penetration estimates for each industry listed in Table 2-1.

Table 2-2. Penetration/Adoption of RBAC

Industry	Current	2003	2006	2009
Example: Banking	***10%***	***65%***	***70%***	***75%***

2.5 ***Technology Choice:*** What factors are most important to your customers in choosing the access control technology they use (e.g., political support, administrative costs, other)?

_____

_____

_____

_____

_____

_____

_____

_____

2.6 How long does it typically take your customers to install and make fully operational a new system with RBAC technology?

_____ months

_____ total person-hours

3. Future Technology Improvements

3.1 What improvements in RBAC technology do you envision occurring in the next 5 to 10 years, and how will they affect implementation costs, annual system administrative costs, and security violations/costs?

RBAC Technology Improvements: _____

_____

_____

Impact on Installation Costs: _____

_____

_____

Impact on Annual System Administrative Costs: _____

_____

_____

Impact on Number and Severity of Security Violations: _____

_____

_____

3.2 What improvements in competing (non-RBAC) technologies do you envision occurring in the next 5 to 10 years, and how will they affect implementation costs, annual system administrative costs, and security violations/costs?

Competing Technology Improvements: _____

_____

_____

Impact on Installation Costs: _____

_____

_____

Impact on Annual System Administrative Costs: _____

_____

_____

Impact on Number and Severity of Security Violations: _____

_____

_____

3.3 Are the technology improvement listed in Questions 3.1 and 3.2 reflected in your RBAC market penetration estimates provided in Table 2-2?

☐ Yes

☐ No—how would your market penetration estimates change?

4. Software Development

As part of our evaluation of the benefits of RBAC, we need to estimate the cost of developing the software tools used by information and system security administrators.

4.1 When did your company first introduce RBAC technology into your software products?

_____ (month/year)

4.2 What was your company's investment in the development of RBAC? If the investment was a joint venture with other companies or educational or governmental agencies (other than NIST), please estimate their total expenditures in developing the technology and indicate the partner.

a. Length of time to develop (months) _____

b. Your company's approximate R&D investment ($) _____

c. Cofunding or R&D expenditures by partner companies ($) _____

4.3 Please comment on what sources aided your development of products and services that incorporate RBAC technology.

4.4 Did your R&D build on concepts and theories available in the professional literature?

☐ Yes

☐ No

4.5 Would your industry have developed an RBAC technology without the availability of concepts and theories in the professional literature?

☐ Yes

☐ No

5. NIST's Contribution to the Development of RBAC

Since 1992, NIST has invested resources in developing and supporting RBAC capabilities.

5.1 Were you aware of NIST's activities?

☐ Yes (go to Question 5.3)

☐ No (go to Question 5.2)

5.2 NIST has developed several RBAC models ranging from $RBAC_0$ to $RBAC_3$. Each model contains greater levels of complexity in terms of constraints and hierarchies. The following table provides a description of the various types of RBAC models.

	Hierarchies	**Constraints**
$RBAC_0$	No	No
$RBAC_1$	Yes	No
$RBAC_2$	No	Yes
$RBAC_3$	Yes	Yes

$RBAC_3$ is the most complex model and is often described as the NIST model. Does your product incorporate the NIST model for RBAC?

☐ Yes

☐ No

5.3 Please estimate the percentage of RBAC developers that incorporate the NIST model into their product?

_____ percent

5.4 Please comment on the impact NIST has had on the development of your company's RBAC technology.

_____

_____

_____

_____

_____

_____

_____

_____

5.5 Has NIST's involvement in RBAC changed the time frame for when RBAC technology has become available for use?

☐ Yes

☐ No

5.6 When do you predict industry would have introduced a software product with comparable capabilities without the aid of NIST?

_____ (year)

5.7 Has NIST's involvement in RBAC increased the penetration rate of the technologies that you described in Table 2.2?

☐ Yes, by how much? (e.g., 5 percent more firms per year will adopt the technology)

_____

_____

_____

_____

☐ No

5.8 Has NIST's involvement in RBAC decreased your development costs?

☐ Yes

☐ No

5.9 If yes, by how much? (e.g., total development costs were 5 percent less)

5.10 Has NIST's involvement in RBAC improved the quality of your product for end users?

☐ Yes, by how much? (e.g., 5 percent easier to move users in and out of roles)

☐ No

5.11 Has NIST's involvement in RBAC changed the type and number of industries that will use RBAC? Please explain.

6. Other Benefits

Please describe other issues that you think are important in assessing the benefits or costs of an access control system.

Thank you for your participation!

Check one or both of the following boxes if you would like to receive a draft and/or final versions on the study:

☐ Yes—please send me a draft version of the report to review prior to publication.

☐ Yes—please send me the final version of the report upon completion of the study.

Appendix B: Questionnaire for Information and System Security Administrators

Questionnaire for Information and System Security Administrators

Introduction

On behalf of the National Institute of Standards and Technology (NIST), Research Triangle Institute (RTI) is investigating the benefits and costs of using role-based access control (RBAC) as an alternative to existing access control techniques. The following specific issues are of interest:

- the administrative costs of establishing and changing user profiles when RBAC or other access control technologies are used;
- the frequency of security violations, both internal and external, when RBAC and other access control technologies are used; and
- the difficulty of altering or changing access control systems.

Our study would benefit a great deal from your input. Please read and consider the enclosed questions as they relate to your company's products. We encourage you to collaborate with your colleagues when answering these questions, because several questions span a variety of aspects of the product design and development process.

Any information you provide will remain strictly confidential. In the published results of this study, information that you provide that is specific to your organization will not be presented explicitly and will not be attributed to your organization, without your permission. Your name will not be shown. However, your organization's name will be acknowledged with appreciation in a list of survey participants.

You may complete the questionnaire online at https://public.rti.org/rbac/. All information transferred electronically will be encrypted. Alternatively, you can e-mail or fax your responses to us at bkropp@rti.org or (919) 541-6683. At any time, if you have any questions, please feel free to contact either Brian Kropp at (919) 485-5584 or Mike Gallaher at (919) 541-5935. Thank you for your input to our study.

1. Contact and Company Information

Contact Name: _____

Company Name: _____

Mailing Address: _____

Title: _____

Phone Number: _____

E-mail: _____

2. Access Control Technologies Used by Your Firm

2.1 In the table below, please identify the access control technologies that your firm or organization uses or has used (or plans to use in the near future), including products that were developed in-house. Please note that if you are currently using an RBAC-based technology we are interested in information on both the RBAC technology and the alternative technology(ies) you are currently using (or have previously used).

Table 2-1. Access Control Technologies in Use (or Used)

Technology	Trade Name	When Installed	Currently in Use
Example: RBAC	***Schumann SAM Tivolie SecureWay***	***1999***	Yes
Example: Identity-Based ACL	***Unix-based systems Web server***	***1995***	No—replaced in 1999

2.2 What factors were important in choosing the access control technology that your firm uses (e.g., political support, administrative costs, others)?

2.3 If your firm currently using multiple access control technologies, what problems have you experienced from the interactions between the technologies?

_____

_____

_____

_____

_____

_____

_____

_____

As part of this study we are interested in the activities a company must undertake to adopt RBAC systems. Typically, before a company can implement an access control technology a period of **system design** must occur. This period consists of creating the system and defining all appropriate roles and the privileges for each of those roles. Following this step, **system implementation** occurs where users are migrated from the previous access control technology to the current technology. Once all users have been placed into the correct roles, **system maintenance** occurs where information and system administrators move users in and out of existing roles as they change roles within the company.

2.4 What best describes you company's current status regarding the use of RBAC systems?

☐ We are considering adopting an RBAC system. (Go to Question 2.5)

☐ We are in the process of designing an RBAC system. (Go to Question 2.5)

☐ We are currently implementing an RBAC system. (Go to Section 3)

☐ We have an RBAC system in operation. (Go to Section 3)

☐ We have no plans to adopt an RBAC system. (Go to Question 2.9)

2.5 Does your company plan to develop an in-house RBAC technology or purchase a commercial system, such as an enterprise management package?

☐ In-house

☐ Commercial system. What package are you considering? _____

2.6 What is your company's projected completion data for implementing the RBAC technology?

_____ month, _____ year

2.7 What is the total number of employees in your firm?

_____ Total number of employees in 1999

2.8 What percentage of those employees are you planning to manage using RBAC technologies?

_____ Percent

(Skip to Section 5)

2.9 Have you investigated the potential use of an RBAC system?

☐ Yes: What were the disadvantages of implementing RBAC?

_____

_____

_____

_____

☐ No

(Go to End)

3. RBAC System Design

For the following questions, please think about the system <u>design</u> phase that your company went through to develop your RBAC-based system. Within this section, the term "custom" design refers to system components that were either developed in-house or were developed specifically for your company by an outside vendor.

3.1 Did your company attempt to develop a custom RBAC system?

☐ Yes (Go to Question 3.2)

☐ No (Go to Question 3.6)

3.2 When did your company first start pursuing the development of a custom RBAC system?

_____ Year

3.3 Was your company successful in developing a custom RBAC-based access control system in-house?

☐ Yes (Go to Question 3.4)

☐ No (Go to Question 3.6)

3.4 What were the total costs of developing the custom technology?

_____ Dollars

3.5 How long did it take to develop the custom technology?

_____ Years

(Skip to Section 4)

3.6 Did your company purchase a commercial RBAC technology?

☐ Yes (for those that responded yes to Question 3.6, go to Section 4, for those that responded no to Question 3.6, go to Question 3.7)

☐ No (Go to Section 4)

3.7 Was your company aware of RBAC technology before you purchased the commercial product?

☐ Yes

☐ No (Go to Section 4)

3.8 Why did your company not pursue a custom-designed RBAC system?

☐ Too costly

☐ Lacked technical skills and knowledge

☐ Other _____

4. System Implementation

For the following questions, please think about the system <u>implementation</u> phase that your company went through in installing your most recent access control technology.

4.1 What is the total number of employees in your firm?

_____ Total number of employees in 1999

4.2 What percentage of those employees are currently managed using RBAC technologies?

_____ Percent

4.3 When you changed from your previous access control technology to RBAC, how long did it take for these employees to be migrated from your old access control technology (e.g., identity-based ACL to RBAC) and what was the level of effort involved?

_____ Months @ _____ person-hours per month

4.4 Did your company purchase any new software or hardware to support the migration to an RBAC technology? What were your expenditures?

_____

_____

_____

_____

_____

_____

4.4a Does the new software you purchased support functions other than RBAC, such as password synchronization or single sign-on functions? If so, please describe these additional functions.

_____

_____

_____

_____

4.5 Did you use a systems integration company to help with installing the RBAC feature? If so, what was their role and approximately what were your expenditures?

4.6 In addition to basic software, hardware, and installation costs, for each change that was made, what other costs (external or internal) did your organization incur associated with transferring from one access control technology to another?

4.7 Do you plan to expand the use of RBAC in the near future?

☐ Yes, expand to _____ percent of employees

☐ No

5. The Benefits and Costs of Maintaining RBAC Systems

For the following questions, please think about the system <u>maintenance</u> phase that your company is currently in.

5.1 For each technology listed in Table 2-1, indicate in Table 5-1 the average time required to complete the following tasks:

a. When a new hire is made, on average, how much time is required to establish his/her user privileges?

b. When an employee changes jobs within the organization, on average, how much time is required to change his/her existing privileges?

c. When an employee changes jobs within the organization, on average, how much time is required to establish new privileges?

d. When an employee leaves the organization, on average, how much time is required to terminate his/her user profile? Please list responses in Table 5-1.

Table 5-1. Time to Complete Tasks

Technology	a. Assigning Existing Privileges to New Users	b. Changing Existing Users' Privileges	c. Establishing New Privileges to Existing Users	d. Termination of Privileges
Example: RBAC	____ ***Minutes***	____ ***Minutes***	____ ***Minutes***	____ ***Minutes***
Identity-based ACL	____ ***Minutes***	____ ***Minutes***	____ ***Minutes***	____ ***Minutes***

5.2 In a typical year, how many times does your company perform the administrative tasks listed in Table 5-1?

a. Assigning Existing Privileges to New Users _____ times/year

b. Changing Existing Users' Privileges _____ times/year

c. Establishing New Privileges to Existing Users _____ times/year

d. Termination of Privileges _____ times/year

5.3 When a new hire is made or a user changes roles, how much downtime does that employee experience while waiting for access to be granted or changed (i.e., how many hours or days is the employee unproductive while waiting for access)? Is the amount of downtime different for RBAC-based systems compared to alternative technology-based systems?

5.4 For each technology listed in Table 2-1, are there any future improvements that you anticipate occurring in the next 5 to 10 years that will affect administrative costs?

5.5 Approximately how many person-hours per year (or full-time staff equivalents) does your company spend on performing access control (authorization) management functions?

_____ hours/year

5.6 What is the average full loaded hourly wage rate of your systems and information security administrative staff?

_____ $/hour

Security Administration

5.7 For each technology listed in Table 2-1, in the first two columns of Table 5-2, please indicate if that technology has ever experienced a security violation and the number of violations per year. In the third column of Table 5-2, please estimate the cost per security violation to the average firm in your industry using each access control technology.

Table 5-2. Security Effects by Access Control Technology

Technology	Security Violation (Yes/No)	Number of Security Violations per Year	Average Cost per Security Violation
Example: RBAC	***Yes***	***X***	***$Y***
Example: Identity-based ACL	***Yes***	***Z***	***$U***

5.8 For each technology listed in Table 2-1, are there any future improvements that you anticipate occurring in the next 5 to 10 years that will reduce the frequency of security violations or the cost per security violation?

6. Other Benefits

6.1 Please describe other benefits or costs that you think are important in assessing the effect of an access control system.

_____

_____

_____

_____

_____

_____

_____

_____

Thank you for your participation!

Check the following box if you would like to receive a final version of the study:

☐ Yes—please send me the final version of the report upon completion of the study.