Towards Security of Integrated Enterprise Systems Management

Alexander D. Korzyk. Sr.
Virginia Commonwealth University
4738 Cedar Cliff Road
Chester, VA 23831
Voice: 804-734-7118
Fax: 804-734-7140
akorzyk@acm.org

ABSTRACT

The global transformation of enterprises using packaged enterprise systems continues at an accelerated rate to support the re-engineering of business processes. This opportunity for structuration requires the sharing of data both within the enterprise and between enterprises in the supply chain. One of the biggest obstacles to integrating data within the enterprise is managing information security. Controlling the access of information continues to be associated with power in the enterprise. The sharing of data once closely controlled will require an integrated enterprise system security management framework to control the access of information (power). The key to allowing communication to occur in an integrated enterprise will be the Extranet. This paper examines current information security literature, proposes architectures for the enterprise system and the management of the enterprise system, and advocates further interpretive research to develop an integrated enterprise system security framework. Failure to use alternative scientific methodologies will make enterprise system research irrelevant.

1. Introduction

Global competition may have caused a dramatic change in the way enterprises structure their organizations. During the 1970s, many large enterprises in the United States came to the brink of bankruptcy. For example, in the auto industry, this was partially caused by the entrance of the Japanese and European automobiles into the United States after the Oil Crisis of 1973. The United States automobile industry had not expected the Japanese automobile industry to be such a major threat. The United States economic posture continued to decline into a severe recession by the end of the 1970s. Many of the large enterprises that survived this economic invasion made strategic decisions during the early to mid-1980s to re-structure their enterprises in order to survive and compete globally. Many of these enterprises have spent over five years and hundreds of millions of dollars implementing or unsuccessfully attempting to implement enterprise systems. Some of the enterprises spend nearly 25% of their entire budgets (Mason 98, p.4) and several have declared bankruptcy in their efforts. It had been conventionally accepted that enterprises spent these outrageous amounts because the enterprise was trying to solve their Year 2000 (Y2K) problem with a rapid Enterprise installation, but as the millenium approaches, enterprises, particularly small to medium size enterprises continue to purchase enterprise system software (Davenport 98, p. 30). Structuration theory (Barley 86, p. 84, Baskerville 96, p. 481), power theory (Tjaden 95, p. 241), Mingers 92, p. 7), and communication theory (Hardwick 96, p. 46), (Ngwenyama and Lee 97, p. 348) each contribute possible explanations of this seemingly irrational behavior of these enterprises. This paper attempts to justify the need for triangulation research. For the past decade, many operations researchers have advocated a new research agenda in addition to the positivist mode with an "integrative view of operations' role in organizations, a wider application of alternative research methodologies, greater emphasis on benefit to the operations manager, cross-disciplinary research with other functional areas, a heavier emphasis on sociotechnical analysis over the entire production system, and empirical field studies" (Meredith, Raturi, Amoako-Gyampah, and Kaplan 88, p. 297).

The introduction of the paper discusses the theoretical basis for enterprise system integration. The second section presents a literature review of enterprise systems, proposes an architecture for enterprise systems and discusses system security. Section 3 conducts a further literature review of enterprise system management, integrates network management with system management to develop an expanded enterprise system management architecture. Section 4 discusses enterprise system security management. The final sections make conclusions and recommend areas for further research and possible case study interview questions.

2. History of Enterprise Systems

Concurrent with the 1970s economic crisis, different rays of hope (silver bullets) appeared in information technology and information systems to enable enterprises to restructure their organizations. Previously, the invention of the integrated circuit and its subsequent miniaturization provided the mechanism for computers to provide better support to business functions by moving the collection of data to the source of the data. The client/server architecture enabled the decentralization of collecting and storing data to the source of the data. Enterprises inserted information technology into their old business processes to automate their business processes until the mid-1980s in mainframe environments (Tjaden 95, p.236). Subsequently, enterprises realized that automation of old business processes did not give the enterprise a competitive advantage to be able to compete globally and moved the old business processes to client/server environments (Nance 96, p. 53). The stock market crash of 1987 may have served as a strong signal to industry to streamline or downsize. Many enterprises made strategic decisions to reengineer business processes and implement custom built software relying on computer aided software-engineering products. As a result, many of these enterprises ended up with stovepipe client/server systems similar to the information systems from the prior decade. Some of the enterprises then realized that their organizations needed to share data not only within the enterprise but share data externally with their supply chain (Dewan 98, p. 221), De 98, p. 98). Enterprise systems management (ESM) facilitates some data integration by providing connectivity and limited translation capabilities to partners in the supply chain (Davenport 98, p. 129), (Hart 91, p. 393), (Hardwick 97, p. 59), (Kateel 96, p. 1001). Enterprises that chose enterprise resource planning (ERP) packages for data integration have faced myriad problems (Berstein 96, p. 86). One of the most glaring problems is that some enterprises are restructuring their business processes to fit the ERP package rather than customizing the ERP package to their custom business process (Gable 98, p. 3, Davenport 98, p. 32). Re-engineering an enterprise based on the ERP package follows from structuration theory because "even identical technologies may occasion different organizational structures in different settings" (Barley 86, p. 84). Regardless of how enterprises implement ERP, ESM will be required to support any ERP implementation strategy. ESM unlike ERP does not require reengineering the enterprise. Rather, ESM allows most enterprises, which implement an ESM product to attempt to integrate the various enterprise systems to some degree. However, in some cases, vendors and enterprises have tried to push ERP systems to perform functions of ESM systems by employing mass customization (Tjaden 95, p. 240).

2.2 Background of Enterprise System Security Management

Since the area of enterprise systems is so vast, this paper will only explore enterprise systems security from a management perspective. Prior to the mid-1990s information security management received little attention from management (Mishina 98, p. 17). However, the sharing of intra-organization and inter-organization data requires collaboration of individuals and organizations (Dewan 98, p. 221). Communication theory addresses the connectivity of computers to networks, which represent individuals and organizations, respectively (Hardwick 96, p. 47). Each individual and organization have a different need to know certain information. Consequently, information security has become of prime importance because even though the data is centrally located, the owners of pieces of the data expect only authorized access to those pieces of data (Divitini 93, p. 181), (De 98, p. 94), (Pritsker 97, p. 36). As some enterprises choose to reverse engineer their business processes, they have become adamant about data access levels (Aiken 98, p. 11). Controlling access to data follows directly from power theory (Tjaden 95, p. 241). The use of enterprise system security management (ESSM) thus involves a combination of structuration, communication, and power theories.

2.3 Enterprise System Literature

The evolution of the enterprise resource planning (ERP) application from material requirements planning (MRP) application continues to evolve. The ERP application has evolved into an enterprise system (ES). "ERP systems offer a fully integrated approach to incorporating a wide range of functional modules (Merit Projecta 98, p. 35). ERP systems are not just implemented as one time or phased projects like other information systems. "An enterprise system is not just a project, it's a way of life" (Davenport 98, p. 30). Manufacturers of enterprise system continue to develop new functional modules for their products. Subsequently, enterprises install the new module. New acquisitions or divested business units will require installations of old and new modules. The modules of an enterprise system necessarily involve the

computing of one module out of many modules. For example the enterprise application modules supported by SAP (Chase, Aqilano, and Jacobs 98, p. 670) are: Sales & Forecasting (SD); Materials Management (MM); Production Planning (PP); Quality Management (QM); Plant Maintenance (PM); Project System (PS); Financial Accounting (FI); Controlling (CO); Plant Asset Management (AM); Human Resources (HR); Workflow (WF); Industry Solutions (IS); and Work bench (WB).

The management parameters of ERP systems interface directly with enterprise system security management (Merit Projecta 98, p. 35): 1) Cross-platform capabilities to manage the business environment in multiple instances from a central console require authorizations; 2) Auto-discovery of ERP resources requires monitoring; 3) Event and resource management requires monitoring audit logs to alert management systems of a perilous condition; 4) ERP systems are mission critical and must rely on database backup and recovery procedures; and 5) ERP systems have a business process orientation which relies on role based security.

2.4 Proposed Enterprise System Architecture (ESA)

ERP systems must be able to work in an architecture such as the one proposed in Table 1. I determined the three stacks of ESA from reviewing the relationships that appear to be operating in complex enterprise systems. An architecture may be constructed to explain the dynamics of the applications involved in enterprise systems. Section 4 will take the proposed ESA and enterprise system management architectures and call for a need to develop a framework to help researchers design specific research studies, interpret existing research, and generate testable hypotheses, which may then be developed into a theory or use existing theories to describe the principles that explain the observed facts (Meredith et al 88, p. 300) of enterprise systems from a management perspective. The ESA has the capability to support numerous modules.

	Enterprise	System	Architecture
Layers	**Database Stack**	**Application Stack**	**Security Stack**
Output Layer	Administration	Job	User
Process Layer	Backup & Recovery	Performance	System
Action Layer	Scheduling	Sizing	Monitoring

Table 1. Enterprise System Architecture

2.5 Enterprise System Security

In addition to Enterprise systems integrating data, management of enterprise systems should integrate network management with systems management. Network management is the management of the web that interconnects all the separate computer systems. A computer system consists of both hardware and software residing on computing device. The hardware of this device could be as large as a mainframe, a mini-computer, microcomputer, or as small as a handheld computer. The software of this device could include an application, database, web browsers, and others graphical user interfaces (GUI). The architectural role of this device could be as a client or as a server. The performance of a mainframe as a server (99.5% availability) is almost double that of a super micro-computer (55 % availability) in terms of fewer outages, less downtime, and better recovery mechanisms (McCune 98, p. 17). The hardware and software used to connect the computer system together form the network. These networks began as local area networks and have continued to expand to global area networks. The hardware consists of such devices as bridges, hubs, routers, firewalls, brouters, digital switches, cables, connectors, modem boards, network interface cards, and other communication cards. The software consists of communication protocol stacks, firewalls, web servers, encryption , guards, etc. The phrase “firewall” applies to the “combination of hardware and software products used to protect the information on your computers from other computers across a network” (Hubel 98, p. 36). Although I have pointed out the differences between network and system management, there are some commonalties of which security is one on which this paper focuses.

3. Enterprise System Management

Network and system management both use intelligent agents that are resident on the hardware device or the software program capturing information much like a flight recorder on a commercial or military aircraft.

Second, network and system management both use a common session layer protocol to communicate information within a system or between systems in a network. The most common management information base used is simple network management protocol (SNMP). Third, both have metaphors for some type of computer-simulated cockpit, which is similar to a commercial or military aircraft cockpit. Some type of read out in the simulated cockpit following the management information format indicates the status of the entire network and all systems contained in that network. The cost savings shown in the Table 2 average approximately $1,000 per user per year (International Data Corporation in Mason 98, p. 3). An enterprise containing 50,000 employees requiring computer access could realize a net savings of $50,000,000 per year. Availability is the reduction of downtime that prevents use of the business application. Enhancement of automation is the value added by automating business management processes. Business process views are a new perspective of the enterprise systems discussed in detail in the following paragraphs.

	Increased Availability	Enhancement of Automation	Business process views	Combined Total
Annualized savings	$3,680	$770	$620	$5,070
5-yr NPV	$14,540	$2,280	$1,600	$20,380

Table 2. Business value from ESM per computer user

3.1 Internet management

Another aspect of network management is Internet management. Most of the concepts discussed earlier apply to the Internet security. Web server management must protect all HTML pages based on user authentication and authorization (Merit Projecta 98, p. 31). An additional concern for network security is not only the Internet (external enterprise network) but also the Intranet (internal enterprise network). Even more of a concern is the Extranet, which combines the users of both the Internet and the Intranet. The Extranet is a communications innovation, which creates an instant electronic supply chain among suppliers and customers globally. The Extranet has the capabilities to allow access to catalogs, purchase orders, invoices, secure e-mail, etc. For example, Ford Motor Company allowed secured access of its Intranet to its entire supply chain one year after it began to allow secured access for Electronic Data Interchange purposes (Austin and Cotteleer 97, p. 1). More than 40% of business to business electronic commerce applications, including electronic data interchange, will be replaced by Extranets in four years and within five years 80% of companies will use Extranets, compared to about 30% in 1998 (Greengard 98, p. 39). One of the most popular implementations of an Extranet is the virtual private enterprise network. The enterprise uses the Internet as a backbone but enterprise also uses encryption between all enterprise nodes on the virtual private network (VPN) to avoid paying the costs of a value added network (VAN).

3.2 Network management

Several operating system manufacturers developed network management products in the early 1990s. These products included Hewlett Packard OpenView, Sun Microsystem Solstice, Sun Microsystem SunNet Manager, IBM NetView, and Cabletron System Spectrum (Steinke 98: 48). These products worked well on each local area network, but could not scale beyond one network. Enterprise network centers looked like the NASA launch space center at Houston with literally hundreds of monitors, one computer and console for each local area network across an entire wall of a computer room, sometimes two or three high.

Operating system (OS) and database management system (DBMS) manufacturers developed server manager software programs for each OS and DBMS. For example, an individual operating the Microsoft Windows New Technology (NT) operating system, may log on a default user account called “administrator” to access server manager programs viewed in a drop-down menu from the common administration selection. Similarly, an individual operating the Oracle DBMS may log on a default user account called “system” to access database administrator programs also viewed in a drop-down menu from the manager selection. Unfortunately, in a client/server environment requires a DBA for each instanciation of a database. Similar to the Houston space center analogy, an enterprise level DBA had to have a console and computer to administer each database instanciation.

3.3 Re-engineering Business Processes

Enterprises have continued to downsize the number of personnel while reengineering business processes during the past ten years. However, enterprises have only downsized and reengineered their computer networks during the past three years because of the recent availability of integrated network and system management products. There are two types of management philosophies, which may form the basis for future development of integrated management. The first principle is based on the business process. A virtual network consisting of all business entities involved in a particular business process can be managed even though components of the virtual network overlap other virtual networks supporting other business processes. For example, take the process of financial accounting. The business accountant needs access to a database containing product information, inventory information, and accounts receivable information.
The business process view rotates from the horizontal to the vertical axis and the traditional resource view from the vertical to the horizontal axis. Instead of the information technology controlling business, the business process controls business (Computer Associates 98, p. 4). In order for the accountant to answer a question about why the cost of a product increased, they must analyze the applications that support financial accounting, the databases and systems the applications use, and the network that connects the applications, databases, and systems.

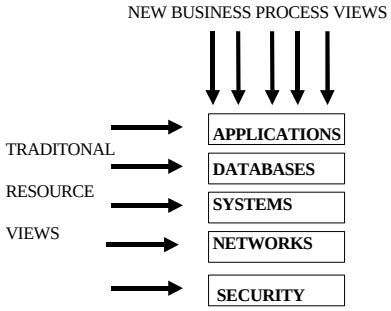


Figure 1. Business Process Principle

The financial accountant could have access to a custom screen with a warning indicator that the customer who had just placed an order with the sales business process has an outstanding balance and is a credit risk based on past payment history so that the customer either makes an immediate payment or is denied the sale. The second principle is based on service level. The sales accountant could have access to a custom screen with warnings or alerts should a stock-out situation be imminent or obsolete products continue to be stocked with no projected orders to guarantee a customer a stable supply of products. "Very few IT organizations have formal service-level agreements (SLAs) with their customers" (Frye 98, p. 34) and the SLAs in place are mostly operational (uptime, system availability). With enterprise systems, management could measure how long it takes a customer to get their sales approved or in this case disapproved. Although only 5% of enterprises currently set SLAs, over 10% should SLAs within a year as more enterprises implement ESM products (Frye 98, p.34). Thus, depending upon the required information, each individual responsible for a business process or service level could have close to real-time access to information if SLAs are met and it adds business value. A puzzle shows the information technology service management that "binds ESM technologies to the company's policies and procedures" (Foster-Melliar 98, see url).

3.4 Enterprise System Management Architecture (ESMA)
Just as I have shown that ES have been astronomically expensive to implement and have taken up to several years to implement, ESM have a similar history of astronomical cost and time consuming implementations. The definition of ESM is "a set of tools and processes designed to help control and operate complex technology in applications it supports" (Merit Projectb 98, Glossary). The following graph shows the slowness of ESM implementation. The data is from the Gartner Group (in Steinke, p.49):

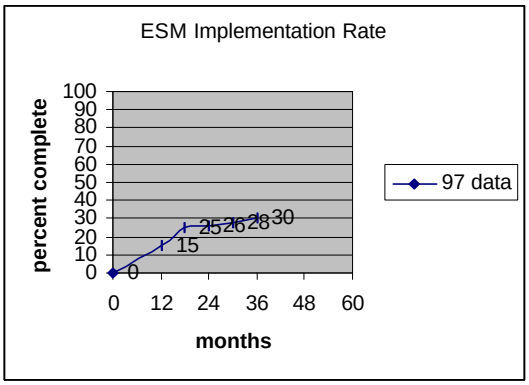


Figure 2 . Enterprise System Management Implementation Rate

The management of an enterprise system necessarily involves the management of the enterprise system as one application out of many applications. The "fundamental goal of security management is to provide a comprehensive security framework that decreases security threats, repulses attacks on an IT infrastructure and secures desktop, application, database, server, and network resources" (Merit Projecta 98, p. 14). The ESMA has the capability to support numerous ES.

	Enterprise	System	Management	Architecture
Layer	**Network Stack**	**Database Stack**	**Application Stack**	**Security Stack**
Output Layer	Configuration	Administration	Job	User
Process Layer	Distribution	Backup & Recovery	Performance	System
Action Layer	Addressing	Scheduling/Replication	Sizing	Monitoring

Table 3. Enterprise System Management Architecture

Although the ESMA shows the application stack as an integral part, the application stack has not been integrated into network management. Figure 3 graphically shows the stack relationships of the ESMA.

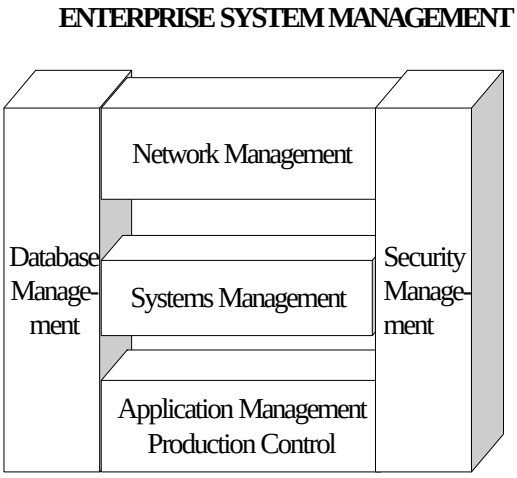


Figure 3. Enterprise System Management Architecture

The application stack by virtue of its nature has been integrated somewhat with systems management. Managing an enterprise from top to bottom requires the ability to track the performance of the application. The database stack tracks the performance of the database, but not the application. The security stack tracks security components of the network and database but not the application. Two ESM software manufacturers have attempted to define the Application Management Specification but have only programmed elementary application programming interfaces. The desktop management task force has yet to address application performance management and error management. The only concepts for implementing application performance and error management involve the rewriting of legacy code. The ESMA should "insulate management applications from the distributed environment by providing a common GUI, object repository, and event services required to create multiple, unified views of the enterprise infrastructure" (Merit Projecta 98, p. 11).

Similar to the concept of components or modules explained for enterprise systems, there are components or modules developed for enterprise systems management. The types of modules available in enterprise system management comes from a product comparison based on one product containing all the modules (Connolly 98, p. 58) in Table 4, which lists eleven modules. The product comparison considered only the top four products. It did not consider other products such as CommandPost made by Boole & Babbage, Inc.

		ESM	PRODUCT	
MODULE	Cabletron Systems **Spectrum**	Computer Associates **Unicenter TNG**	Hewlett-Packard **OpenView**	Tivoli Systems **Enterprise**
Desktop Mgmt	Yes	Yes	Yes	Yes
Software distribution	No	Yes	Yes	Yes
Inventory	No	Yes	Yes	Yes
Application Mgmt	No	Yes	Yes	Yes
Server Mgmt	No	Yes	Yes	Yes
Reporting	Yes	Yes	Yes	Yes
Security	No	Yes	Yes	Yes
Remote configuration	Yes	Yes	Yes	No
Network Mgmt	Yes	Yes	Yes	Yes
Backup	No	Yes	Yes	No
Programming tools	Yes	No	Yes	Yes
Customization tools	Yes	Yes	Yes	Yes

Table 4. ESM Product Comparison by Module

4. Enterprise System Security Management

This section will examine the security stack of the ESMA. The security stack includes user administration, system security, and monitoring for violations. "Security products must communicate with each other in order to exchange information about users, data, and resources," (Merit Projecta 98, p. 14). User administration is normally the daily responsibility of a security administrator. Unfortunately, the security administrator often is also the system administrator, the network administrator, and sometimes even the database administrator. The focus routinely ends up on keeping the system running rather than on security especially if there are only one or two personnel. The security administrator tries to ensure that userids and passwords are properly assigned, authorized permissions enforced, and that each person only sees that information which they need to know. Security administrators spend much of their time determining the read, write, update, and delete permissions for files and directories. Even for a relatively small size network, "the chore of identifying and naming resources can be mind-numbing" (Willis 98, p. 50). The security policies are developed by the human security managers and programmed in the security management software. Even if an enterprise began with one equipment manufacturer for all if its computers, within a three-year period the enterprise would become a heterogeneous environment. In the

past, security managers and security administrators operated in a homogeneous environment. For example, twenty years ago, a typical enterprise had a very large IBM mainframe, IBM communication devices, and IBM dumb terminals. The security manager on the mainframe set security policy and the security administrators dealt mostly with physical security and password security in the user's area. Today, mainframes are still cast in the electronic business role to make its data readily accessible in many cases by connecting the mainframe as the back ends of an Intranet or Extranet (McCune 98, p. 18). Security policy is still set by the security manager on the mainframe just as during the last 30 years of mainframe computing.

4.1 Combining Network and System Security

Perhaps the most important security aspect in managing an enterprise system is combining network security with system security. Security risk analysis literature began to appear shortly after the first computer systems established networks with other computers to produce knowledge about the security of a networked system under development (Baskerville 96, p. 484). Network security must control, audit, and restrict access, based on userid, to all systems on Internet/Intranet networks by enabling network security policies and rules to be centrally defined and enterprise-wide enforced (Merit Projecta 98, p. 15). The enterprise system managers of today offer a significant convenience to the user in terms of accessing different systems within the enterprise system. Security management should be enterprise-aware. "Your firewall is the most important security measure you can take to protect your business on the Internet" (Hubel 98, p. 36).

4.2 Security Features

Many pre-enterprise systems require the user to memorize several passwords and sometimes, different userids. This feature is called single sign-on. The user only needs to know one userid and one password to gain access to all their authorized files, databases, reports, and directories. The screen, which the user initially sees upon logging on to the system, is determined by the security policies, group membership, database role, and access privileges. Users should not have to be re-defined between multiple systems. When a security event occurs anywhere in the enterprise, information about the event should be obtained and appropriately reported to security administrators, and, if it is serious, to the security managers. In a survey of enterprises, which implemented single sign-on, the average annual cost savings directly attributable to SSO was $50 per user (Mason 98, p. 3). So an enterprise consisting of 50,000 employees with computer access could possibly realize an annual net savings of $2.5 million. Centralized anti-virus management is also a critical to security management because over 90% of enterprises have lost data or had data corrupted due to a virus attack because viruses can pass across the network and from computer to computer (Merit Projecta 98, p.16). Virus protection includes real time detection and cure of viruses, automatic monthly updates for new viruses, automatic virus scanning, virus source tracking, and a virus wall. Table 5 using data from the 1997 IDC survey shows some of the cost savings from enterprise system security management.

Security Issues	ESSM	Pre-ESSM	Reduction of staff hours	Cost savings per user per year
Security violations	2 hours	16 hours	14 hours	$87
Virus infections	11 hours	43 hours	32 hours	$203
Single Sign-On	2 hours	10 hours	8 hours	$50
Totals	13 hours	59 hours	46 hours	$340

Table 5. Enterprise System Security Management Cost Savings

Another feature not yet fully incorporated in ESM software is that of unitary logon. This feature would allow a user to logon to any computer in the enterprise to and use any authorized application. The latest release of one ESM product allows administrators the capability to manage resources from anywhere on the enterprise network by using Java interfaces to launch the management console from any Java-enabled web browser (Hurwitz 98, p.1).

4.4 Object-oriented Security

Future development may include a movement to object-oriented repositories to specify "management policies that can proactively adjust management settings in addition to automatically launching corrective actions" (Merit Projecta 98, p. 8). The enterprise system management framework should include an object repository (Yankee 97, p.2).

Another use of an object is as an intelligent agent that can predict both near-term and future outcomes, which in turn trigger changes in security policies real-time, by recognizing a pattern of system behavior. This concept has been partially accomplished by the use of neural networks and intelligent agents called a neugent which uses the metaphor of a VCR remote control to allow the user to fast forward or reverse a situation (Aberdeen 98, p. 2). The common object repository is shown in detail in Figure 4 (based on Computer Associates 98, p. 7). The top tier is the user interface layer. The second tier is the common object repository and databases connected to it. The third tier is the enterprise system management layer, which reflects the four stacks described in Table 4. Enterprise System Management Architecture. The bottom layer is the intelligent agent layer. The security agent, for example, can share data with other peer agents, perform filtering, monitor other managers, and provide automatic responses to alerts.

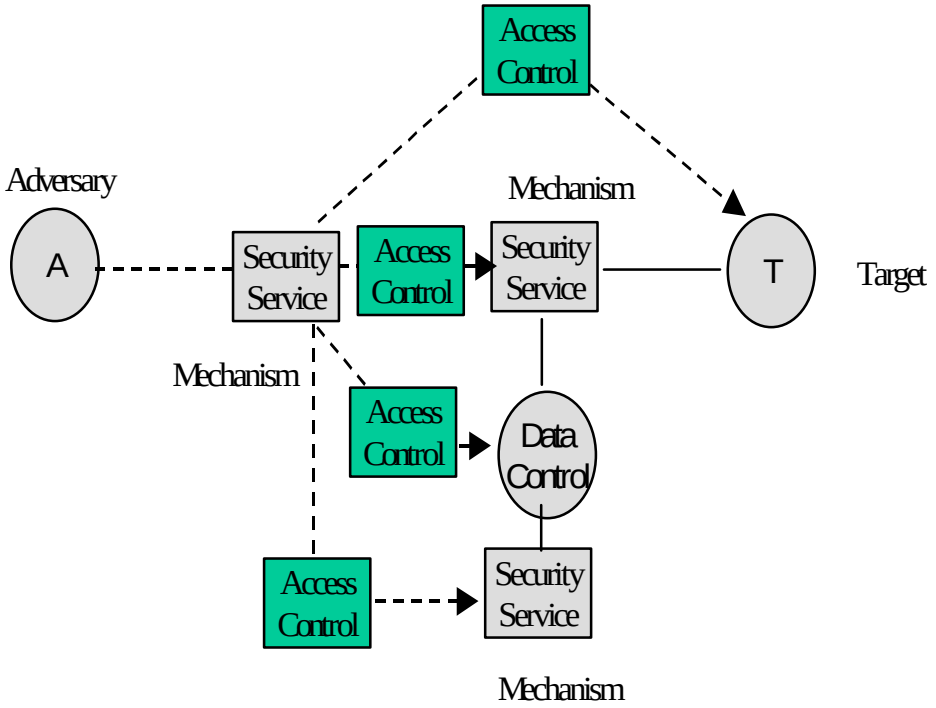


Figure 4. Enterprise Management with Intelligent Agents and Common Object Repository

5. Conclusions

Enterprises are transforming from industrial age automation to information age enterprise systems at an accelerating rate in order to survive into the next millennium. The global transformation of enterprises using packaged enterprise systems continues at an astounding rate and astronomical costs to support the re-engineering of business processes. Many enterprises have used the insertion of enterprise system software packages to structure their enterprise through a commonly know phenomenon called business process re-engineering. This opportunity for structuration requires the sharing of data both within the enterprise and between enterprises in the supply or value chain. One of the biggest obstacles to integrating data within the enterprise is managing knowledge. Controlling the access of information continues to be associated with power in the enterprise. The sharing of knowledge, information, and data once closely controlled will require an integrated enterprise system security management framework to satisfactorily control the access

of information (power). The key to allowing the communication of information to occur in an integrated enterprise will be the Extranet. This paper examines current information security literature, proposes architectures for the enterprise system and the management of the enterprise system, and advocates further interpretive research to develop an integrated enterprise system security framework. Failure to use alternative scientific methodologies to develop an integrated enterprise system security management framework will make enterprise system research irrelevant.

6. Recommendations for Further Research

6.1 Development of an object-oriented ESSM Security Framework

In order to avoid the possibility of performing irrelevant research such as was done for 20 years in operations management (Meredith et al 88, p. 320), researchers must employ research paradigms used in other scientific disciplines. One such scientific methodology successfully used by other scientific disciplines is the field study.

6.2 Conduct a field study.

Suggested interview questions by major topical area:

1. Product selection
    - Why did your enterprise need ESM?
    - What were the objectives of implementing ESM?
    - How did you select one ESM?
    - Which features were requirements?
    - Did you sacrifice any features?
2. Installation and implementation
    - How long did it take or how long is it taking?
    - Did you use a consultant?
    - Did you experience downtime?
    - Did any feature become more important after it was installed?
    - Did you have to upgrade any hardware?
    - How did you handle new issues?

3. Interoperability with third party products
    - What third party products do you use?
    - Was it difficult to install and configure the third party products?
    - Do you need a third party management product?
    - Did you consider third party products when you selected your ESM product?
    - Did the ESM product provide for everyone?

4. Support and training by vendor
    - What type of maintenance agreement did you get?
    - Did you receive any product training?
    - Where did you receive the product training?
    - Was the training adequate?
    - Was the training customized for your enterprise?

5. Total cost of ownership
    - What is the profile of each user to include salary, usage, proximity to computers?
    - Is someone always available to help users?
    - How many staff positions did you cut?
    - How much do you spend on the ESM software and hardware?
    - What was the total implementation cost to include consultant fees?
    - What costs are you saving by using ESM?

6. Structural changes of the enterprise
    - Did your enterprise re-engineer any processes at the same time?
    - Was a new position created to install and subsequently manage ESM?
    - At what level of the enterprise is the position?
    - Did your enterprise already have an ES?
    - How much is your enterprise geographically dispersed?

7. Security
    - Did you use role-based access control?
    - How did you integrate network security?
    - Did you purchase any separate network security products for intrusion detection and monitoring or any other security function?
    - How do you manage Internet security?
    - Do you require security background investigations for your personnel?
    - How do you separate different levels of sensitive data?

8. Lessons learned
    - Did you learn anything about your enterprise during the entire process?
    - Were changes in the enterprise planned?
    - Was the implementation successful and complete?
    - What is the overall satisfaction with the new capabilities?
    - What could others learn by your mistakes?

REFERENCES

Aberdeen Group, "Computer Associates' Unicenter TNG Enters the Next Dimension". url://www.cai.com/analyst/111/, 11/14/98, pp. 1-3.

Aiken, Peter; Ngwenyama, Ojelanki K.; and Broome, Lewis. "Improving Implementation Productivity by Reverse Engineering New Systems." Submitted to *IEEE Software*, September 1998, pp. 1-14.

Austin, Robert D. and Cotteleer, Mark. "Ford Motor Company: Maximizing the Business Value of Web Technologies." *Harvard Business School Case*, 9-198-006, July 10, 1997, pp. 1-14.

Barley Steven, "Technology as an Occasion for Structuring: Evidence from Observations of CT Scanners and the Social Order of Radiology Departments," *Administrative Science Quarterly*, Volume 31, March 1986, pp. 78-108.

Baskerville, Richard L. and Stage, Jan. "Controlling Prototype development Through Risk Analysis." *MIS Quarterly*, Volume 20, Number 4, December 1996, pp. 481-504.

Berstein, Philip A. "Middleware: A Model for Distributed System Services." *Communications of the ACM*, Volume 39, Number 2, 1996, pp. 86-98.

Chase, Richard B.; Aquilano, Nicholas J.; and Jacobs, F. Robert. *Production and Operations Management: Manufacturing and Services*, 8th Edition. Irwin McGraw-Hill: New York, New York, 1998, pp. 624-677.

Computer Associates. "Enterprise Management Strategy: Managing the Enterprise". url://www.cai.com/products/unicent/whitepap.htm, 11/14/98, pp. 1-15.

Connolly, P.J. "Product Comparison Enterprise Network Management". *LANTIMES*, October 12, 1998, pp. 52-58.

Davenport, Thomas H. "Living With ERP". *CIO*, Volume 12, Number 5, December 1, 1998, pp. 30-32.

Davenport, Thomas H. "Putting the Enterprise into the Enterprise System." *Harvard Business Review*, July-August 1998, pp. 121-131.

De, Prabuddha; Ferratt, Thomas W. "An Information System Involving Competing Organizations". *Communications of the ACM*, Volume 41, Number 12, December 1998, pp. 90-98.

Dewan, Sanjeev; Michael, Steven C.; Min, Chung-ki. "Firm Characteristics and Investments in Information Technology: Scale and Scope Effects". *Information Systems Research*, Volume 9, Number 3, September 1998, pp. 219-232.

Divitini, Monica; Omodel Sale, Giuseppe; Pozzoli, Alberto; and Simone, Carla. "Supporting the Dynamics of Knowledge Sharing within Organizations." *COOCS '93*, ACM California, November 1993, pp. 178-183.

Foster-Melliar. "IT Service Management", url://www.foster-melliar.com/puzzle.htm. 9/26/98.

Frye, Colleen. "Managing R/3". *Software Magazine*, August 1998, pp. 31-35.

Gable, Guy G. "Large Package Software: a Neglected Technology?" *Journal of Global Information Management*, Volume 6, Number 3, 1998, pp. 3-4.

Greengard, Samuel. "Extranets, The e-business Link". *Beyond Computing*, Volume 7, Number 5, June 1998, pp. 38-41.

Hardwick, Martin and Bolton, Richard. "The Industrial Virtual Enterprise." *Communications of the ACM*, Volume 40, Number 9, September 1997, pp. 59-60.

Hardwick, Martin; Spooner, David L.; Rando, Tom; and Morris, K.C. "Sharing Manufacturing Information in Virtual Enterprises." *Communications of the ACM*, Volume 39, Number 2, February 1996, pp. 46-54.

Hart, Paul and Estrin, Deborah. "Inter-Organization Networks, Computer Integration, and Shifts in Interdependence: The Case of the Semiconductor Industry." *ACM Transactions on Information Systems*, Volume 9, Number 4, October, 1991, pp. 370-398.

Hubel, Martin. "Under Lock and Key". *DB2 Magazine*, Volume 2, Number 3, Winter 1997, pp. 34-37.

Hurwitz, Judith. "Unicenter TND: It's About Time" url://www.cai.com/analyst/108/ . Hurwitz Group, April 1998.

Kateel, Ganesh.; Kamath, Manjunath; and Pratt, David. "An Overview of CIM Enterprise Modeling Methodologies." *Proceedings of the 1996 Winter Simulation Conference*, 1996, p. 1000-1007.

Mason, Paul. "Creating Business Value from Integrated System Management". url://www.cai.com/merit/compas/compas.htm, pp. 1-9.

McCune, Jenny. "The Mainframe Meets the Web". *Beyond Computing*, Volume 7, Number 6, July/August 1998, pp. 17-20.:

Meredith, Jack R.; Raturi, Amitabh; Amoako-Gyampah, Kwasi; and Kaplan, Bonnie. "Alternative Research Paradigms in Operations," *Journal of Operations Management*, Volume 8, Number 2, October, 1989, pp. 297-325.

Merit Projecta. "Best Practices in Enterprise Management". The Maximizing Efficiency of Resources in Information Technology Project, June 1998, pp. 1-43.

Merit Projectb. "Defining the Business Value of Enterprise Management". The Maximizing Efficiency of Resources in Information Technology Project, June 1998, pp. 1-Glossary.

Mingers, John. "Recent Developments in Critical Management Science." *Journal of the Operational Research Society*, Volume 43, Number 1, 1992, pp. 1-10.

Mishina, M. "Connectivity Creates Security Headaches." *AS/400 Systems Management*, Volume 26, Number 5, 1998, pp. 16-19.

Nance, William D. "An Investigation of Information Technology and the Information Systems Group as Drivers and Enablers of Organizational Change." *SIGCPR/ SIGMIS '96*, ACM, Denver Colorado, 1996, pp. 49-57.

Pritsker, Kenneth D. "Strategic Reengineering: An Internal Industry Analysis Framework." *SAM Advanced Management Journal*, Autumn 1997, pp. 32-43.

Steinke, Steve. "In Search of Integrated Management". *Network Magazine*, Volume 13, Number 13, December 1998, pp. 48-51.

Tjaden, Gary S. "Measuring The Information Age Business." *Technology Analysis and Strategic Management*, Volume 8, Number 3, 1996, pp. 233-246.

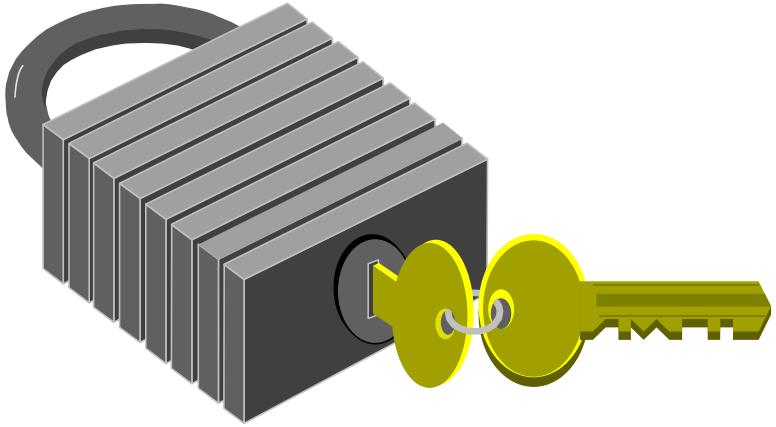
Willis, David. "Finally! A Light at the End of the Tunnel". *Network Computing*, Volume 9, Number 22. December 1, 1998, pp. 48-66

Yankee Group. "CA World '97: Enterprise Management Blitzkrieg". *Client/Server Computing Module* url://www.cai.com/products/unicent/analyst7/yankee.htm, Volume 12, Number 10, August 1997, pp. 1-3.

Enterprise System Management

J. G. Van Dyke & Associates

Virginia Commonwealth University



Towards Security of Integrated Enterprise Systems Management

by

Alexander D. Korzyk, Sr.

Enterprise System Management

J. G. Van Dyke & Associates

Agenda

Virginia Commonwealth University

- Introduction
- Enterprise Systems and Business Process Re-engineering
- Development of Enterprise System Management
- Enterprise System Security Management
- Recommendations for further research
- Sample interview questions

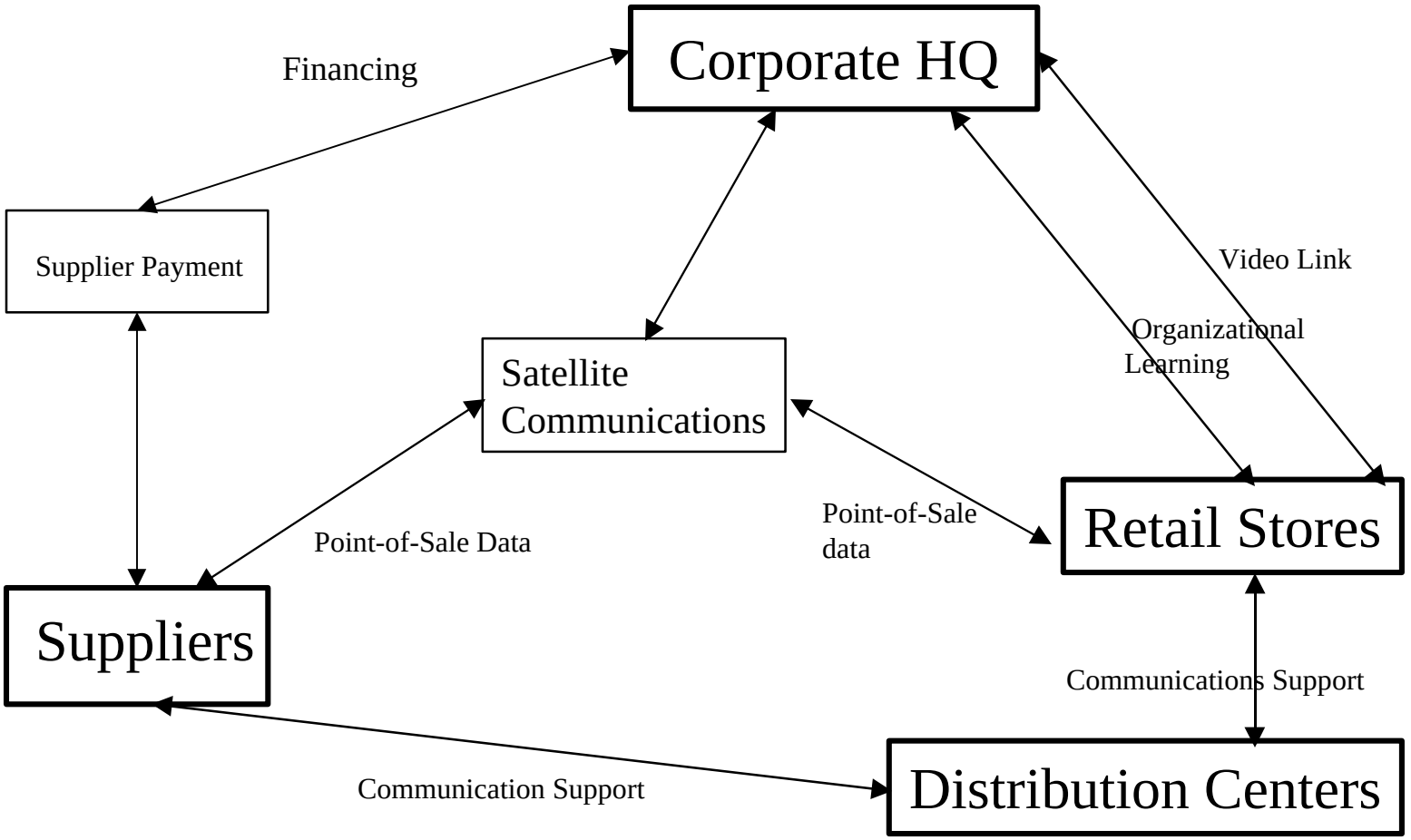
Enterprise System Management

- Apply a *total systems* approach to managing the enterprise network and all computer systems
  - information
  - materials
  - and services

Enterprise System Management
WALMART Extranet

J. G. Van Dyke & Associates

Virginia Commonwealth University



Enterprise System Management

Business Process Reengineering

J. G. Van Dyke & Associates

Virginia Commonwealth University

- "Reengineering is the ***fundamental*** rethinking and ***radical*** redesign of business ***processes*** to achieve ***dramatic*** improvements in critical, contemporary measures of performance such as cost, quality, service, and speed."

Source: Hammer, Michael and James Champy (1993) *Reengineering the Corporation: A Manifesto for Business Revolution*. New York: Harper

Enterprise System Management

- Fundamental
  - *Why* do we do what we do?
  - Ignore *what is* and concentrate on *what should be.*
- Radical
  - Business *reinvention* vs. business improvement

Enterprise System Management

Principles of Reengineering

- Organize around outcomes, not tasks
- Have those who use the output of the process perform the process
- Merge information-processing work into the real work that produces the information
- Treat geographically dispersed resources as though they were centralized

Enterprise System Management

Principles of Reengineering

- Link parallel activities instead of integrating their results
- Put the decision point where the work is performed, and build control into the process
- Capture information once--at the source

Enterprise System Management

SD	Sales & Forecasting
MM	Materials Management
PP	Production Planning
QM	Quality Management
PM	Plant Maintenance
PS	Project System
FI	Financial Accounting
CO	Controlling
AM	Plant Asset Management
HR	Human Resources
WF	Workflow
IS	Industry Solutions
WB	Work bench

Enterprise System Application Modules

Enterprise System Management

J. G. Van Dyke & Associates

Virginia Commonwealth University

	Enterprise	System	Architecture
Layers	**Database Stack**	**Application Stack**	**Security Stack**
Output Layer	Administration	Job	User
Process Layer	Backup & Recovery	Performance	System
Action Layer	Scheduling	Sizing	Monitoring

Enterprise System Architecture

Enterprise System Management

J. G. Van Dyke & Associates

Virginia Commonwealth University

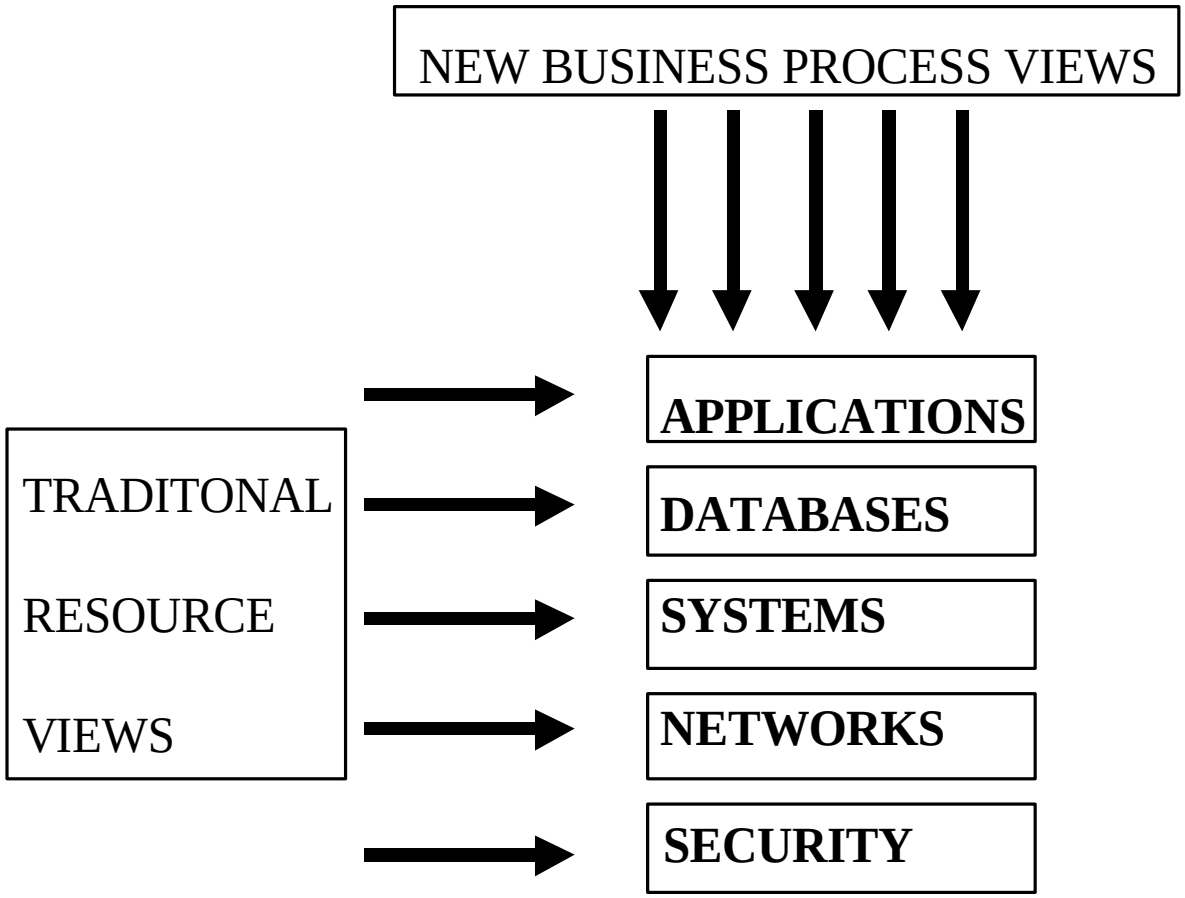
	Increased Availability	Enhancement of Automation	Business process views	Combined Total
Annualized savings	$3,680	$770	$620	$5,070
5-yr NPV	$14,540	$2,280	$1,600	$20,380

Business Value ($ saved per User)

Enterprise System Management

J. G. Van Dyke & Associates

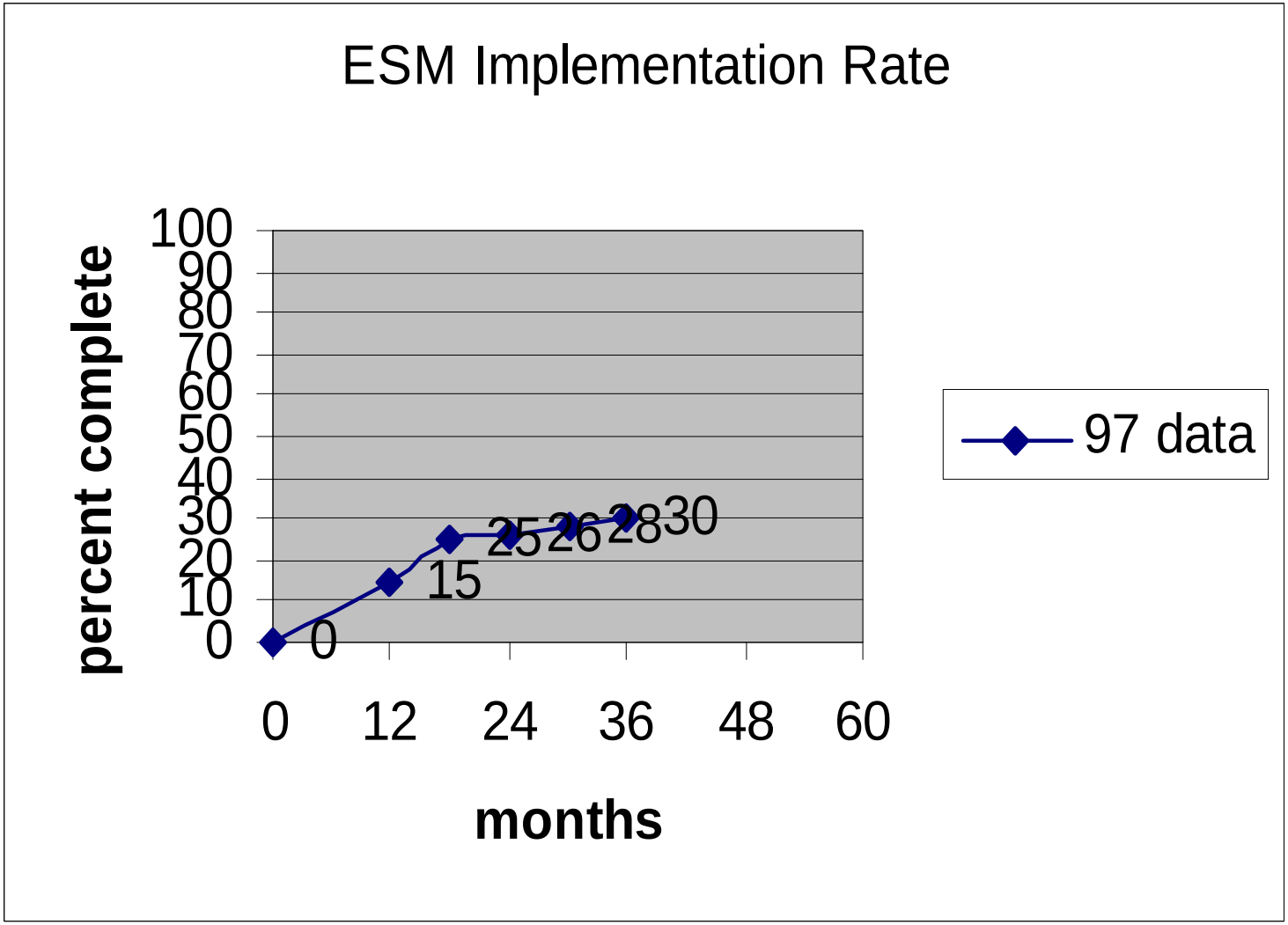
Virginia Commonwealth University



Enterprise System Management

J. G. Van Dyke & Associates

Virginia Commonwealth University



Enterprise System Management

J. G. Van Dyke & Associates

Virginia Commonwealth University

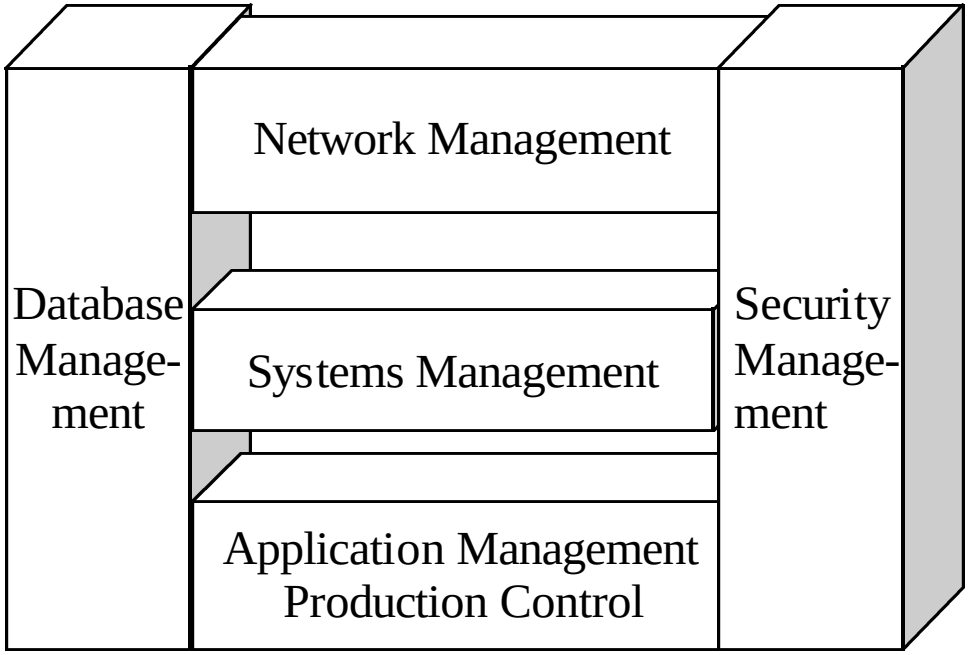
	Enterprise	System	Management	Architecture
Layer	**Network Stack**	**Database Stack**	**Application Stack**	**Security Stack**
Output Layer	Configuration	Administration	Job	User
Process Layer	Distribution	Backup & Recovery	Performance	System
Action Layer	Addressing	Scheduling/Replication	Sizing	Monitoring

Enterprise System Management Architecture

Enterprise System Management

J. G. Van Dyke & Associates

Virginia Commonwealth University



Enterprise System Management Architecture

Enterprise System Management

J. G. Van Dyke & Associates

Virginia Commonwealth University

		ESM	PRODUCT	
MODULE	Cabletron Systems **Spectrum**	Computer Associates **Unicenter TNG**	Hewlett-Packard **OpenView**	Tivoli Systems **Enterprise**
Desktop Mgmt	Yes	Yes	Yes	Yes
Software distribution	No	Yes	Yes	Yes
Inventory	No	Yes	Yes	Yes
Application Mgmt	No	Yes	Yes	Yes
Server Mgmt	No	Yes	Yes	Yes
Reporting	Yes	Yes	Yes	Yes
Security	No	Yes	Yes	Yes
Remote configuration	Yes	Yes	Yes	No
Network Mgmt	Yes	Yes	Yes	Yes
Backup	No	Yes	Yes	No
Programming tools	Yes	No	Yes	Yes
Customization tools	Yes	Yes	Yes	Yes

Product Comparison by Module

Enterprise System Management

J. G. Van Dyke & Associates

Virginia Commonwealth University

Security Issues	ESSM	Pre-ESSM	Reduction of staff hours	Cost savings per user per year
Security violations	2 hours	16 hours	14 hours	$87
Virus infections	11 hours	43 hours	32 hours	$203
Single Sign-On	2 hours	10 hours	8 hours	$50
Totals	13 hours	59 hours	46 hours	$340

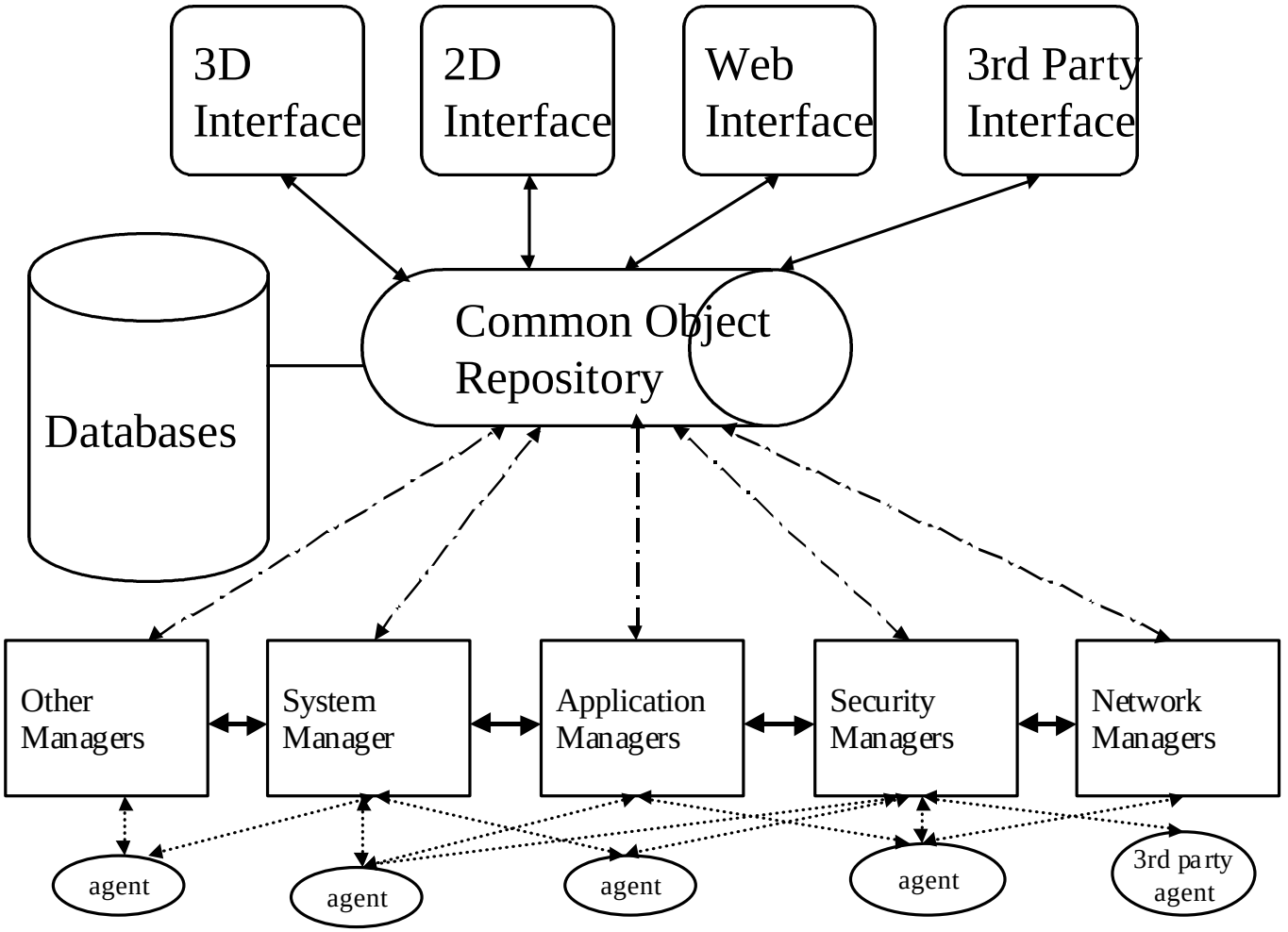
Enterprise System Security Management
Cost Savings

Enterprise System Management

Object-Oriented ESM

J. G. Van Dyke & Associates

Virginia Commonwealth University



Enterprise System Management

- Benefits of ESM Software
  - Reduce system costs
  - Reduce number of tools
  - Simplify operations
  - Simplify training
  - Enhance consistency
  - Enhance security
  - Improve software distribution

Enterprise System Management

- Availability Management
  - Enterprise wide view across all platforms
  - Enterprise wide fault management focal point
  - Enterprise wide service delivery view
  - Enterprise wide support for the infrastructure

Enterprise System Management

- Service Management
  - Directory service
    - » Authentication
    - » Access control
    - » Configuration

Enterprise System Management

- Network Services
  - Move to proactive
  - Focus on business process views
  - Desired state management
  - Real-time analysis of problems
  - Reduce complexity
  - Integrate security

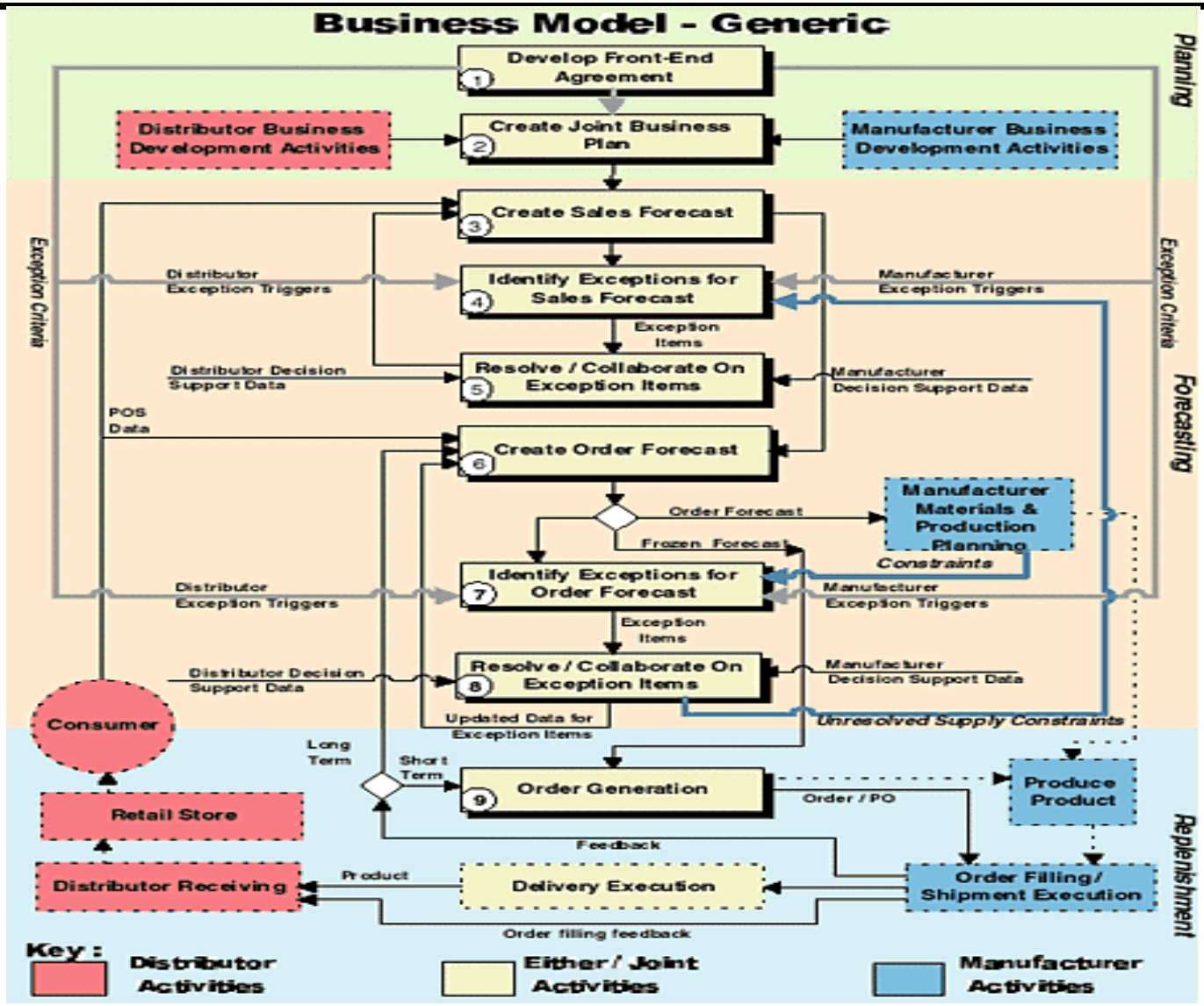
Enterprise System Management

- Assess the complexity
- Assess the risk
- Quantify the total cost of ownership
- Determine the useful life cycle
- Determine benefits
- Calculate ROI

Enterprise System Management
Enterprise System Business Model

J. G. Van Dyke & Associates

Virginia Commonwealth University



Enterprise System Management

- Conclusions
  - Packaged vs Customized Enterprise Systems
  - Business Process Reengineering Renamed
  - Value Chain Data Sharing
  - Knowledge Management
  - Extranet

Enterprise System Management

- Recommendations for Further Research
  - Development of object-oriented ESSM Framework
  - Cross ESM Integration
  - Conduct Field Studies

Enterprise System Management

J. G. Van Dyke & Associates

Virginia Commonwealth University

- Sample Topical Questions for a Field Study
  - Why was this particular ESM selected?
  - How did you install and implement the ESM?
  - Did the ES inter-operate with third party products?
  - What testing or training was conducted?
  - Did the Total Cost of Ownership decrease?
  - What structural changes occurred in the enterprise?
  - How do you manage enterprise security?
  - What lessons learned could benefit other enterprises?