

Security Analysis of Internet Technology Components Enabling Globally Distributed Workplaces - A Framework

MANISH GUPTA

M&T Bank Corporation, Buffalo, NY, USA

SHAMIK BANERJEE

Conagra Foods Inc., Omaha, Nebraska, USA

MANISH AGRAWAL

University of South Florida, Tampa, Florida, USA

and

H.RAGHAV RAO

State University of New York, Buffalo, NY, USA

As organizations increasingly operate, compete and cooperate in a global context, business processes are also becoming global to generate benefits from coordination and standardization across geographical boundaries. In this context, security has gained significance due to increased threats, legislation and compliance issues. This paper presents a framework for assessing the security of Internet technology components that support a globally distributed workplace. Four distinct information flow and design architectures are identified based on location sensitivities and placements of the infrastructure components. Using a combination of scenarios, architectures and technologies, the paper presents the framework as a development tool for information security officers to evaluate the security posture of an information system. To aid managers in better understanding their options to improve security of the system we also propose a 3 dimensional representation based on the framework, for embedding solution alternatives. To demonstrate its use in a real-world context, the paper also applies the framework to assess a globally distributed workforce application at a northeast financial institution.

Categories and Subject Descriptors: K.6.5 [**Computing Milieux**]: Management of Computing and Information Systems – *Security and Protection*; H.1.m [**Information Systems**]: Models and Principles – Miscellaneous; K.4.4 [**Computers and Society**]: Electronic Commerce – *Security*; C.4 [**Computer-Communication Networks**]: Performance of Systems – *Measurement Techniques, Reliability, Availability and Serviceability*.

General Terms: Security, Measurement, Reliability, Management

Additional Key Words and Phrases: Security Analysis, Globally Distributed Workforce, Internet Applications, Risk Management.

1. INTRODUCTION

Global competition has increased the pressure on organizations to reduce turn-around-time to market for their products and services. Concepts such as the 24/7 knowledge factory have been introduced to leverage these environments where globally distributed work (GDW) teams can work on specific endeavors round the-clock [Seshasai, et al. 2006]. Information systems play a key role towards achieving this goal by linking globally distributed workplaces and work-teams. The globally distributed workplace describes work teams, most commonly in software development and e-commerce, working on projects from locations distributed across companies and across the globe.

e-Commerce and software systems have evolved over the years using technologies which have enabled handling of diverse critical applications. As component based designs gain popularity and security concerns rise on the information highway, it has become increasingly important to analyze the software architecture components for security evaluation. The need for quantifying security of software systems, for example through vulnerability identification, is gaining importance with many mission critical applications being accessed across the oceans [Sharma and Trivedi 2005]. The utility of architectural frameworks to manage and optimize security in an escalating threat environment had never been more [Axelrod 2007]. A rigorous analytical dissection of the architecture will help reduce the vulnerability of the overall system, ensuring a secured environment.

It is highly imperative that entire E-commerce environment be constructed from components that recognize the need for security services and provide means for security integration, administration, and management [Gupta, et al. 2004]. In this paper, we analyze the security of information system architectures, particularly based on internet technology components, that are used to serve e-commerce and software systems based on their functional properties. The architecture of a system determines the way the different components interact and is a major factor contributing to the way the system behaves and enables information sharing across geographical boundaries [Gokhale and Trivedi 2002, Goseva-Popstojanova, et al. 2001, Goseva-Popstojanova and Trivedi 2001]. The topologies of the architectures vary based on the distributiveness of the application processes, data repositories and the operational interdependencies. In developing the analysis framework, we follow a prior development of a comprehensive threat analysis model that has been used by the authors in the analysis of detailed transactional workflows to expose the vulnerabilities that are prevalent in electronic bill payment systems [Tanna, et al. 2005].

The framework outlined in this paper delves into a greater depth of analysis into roles and forms of components as they are defined in an architectural design of an information system. The identification of high-risk components is particularly important for independent verification & validation (IV&V) processes. We use component analysis to develop the framework based on the independent and static complexity of the primitive components and connectors that form the high-risk components. The static complexity at the architecture level is obtained by applying functions described in this paper for combining the static complexities of its primitive parts [Goseva-Popstojanova, et al. 2001]. Our framework utilizes subjective evaluations and uses tacit knowledge

(experience, rule of thumb) to assess indices to describe the security posture of a firm [Ekanayaka, et al. 2002]. The formulation and implementation of IT strategy via a robust architecture for web-enabled environments is critical [Hagel III and Brown 2001], particularly when using multiple vendors providing applications solutions across different business processes [Broadbent, et al. 1999].

The contributions of the paper include the following. The proposed detailed framework affords a map to assess the security of IT infrastructure servicing business needs in the context of GDW or an outsourcing arrangement. The framework includes analyses of various aspects of a GDW system – the technology components, access channels, architecture and threats. The real-world validation of the framework, achieved through application at a financial institution in the north-east US, lends shows the applicability of the framework in security assessment. This paper also provides a 3-dimensional solution map, that can be used as a more fine-grained structure for evaluating the threats to a firm in a globally distributed workplace.

The paper is organized as follows: Section 2 presents the basic concepts and definitions for risk assessment methodologies. Section 3 classifies Internet technology components and compares the relative security merits of components as they interact in globally distributed information systems. Section 4 presents information access channels and their distribution and composition from a security assessment standpoint. Section 5 presents the component distribution focusing on the spatial distribution of components. Using these building blocks, in Section 6, we propose a framework to analyze security strengths of an information system used in a globally distributed enterprise. A real-world application of the framework is presented to operationalize the framework and a 3-dimensional representation provides insights into approaches available to managers to improve information security. Finally section 7 concludes the paper.

2. INFORMATION SYSTEMS CLASSIFICATION FOR SECURITY ASSESSMENT

International outsourcing has necessitated the sharing of information across globally distributed workplaces, including across organizations[Pawlowski 2000]. Virtual teams have enabled globalization of the business environment and distant collaborative teams. Such teams are groups of geographically and organizationally dispersed knowledge workers brought together across time and space through information and communication technologies on an ‘as needed basis’ in response to specific customer needs or to complete unique projects [Jarvenpaa and Leidner 1999]. For example, the authors have

insight into a major multi-national corporation that is expected to reach revenues of \$ 1 Bn by 2008 by providing offshore services both internally to the different divisions of the multinational as well as other clients from all over the globe. The corporation uses global work teams whose members speak 19 languages and delivers services from 16 operations centers in the United States, Mexico, Hungary, Romania, India and China. At the highest level, such firms offer a menu of services such as network management and application maintenance. To provide such services, they use an IT infrastructure similar to Figure 1, which forms the basis for the framework proposed herein. Though names and locations have been disguised to maintain confidentiality, the figure has been adapted from a real organization.

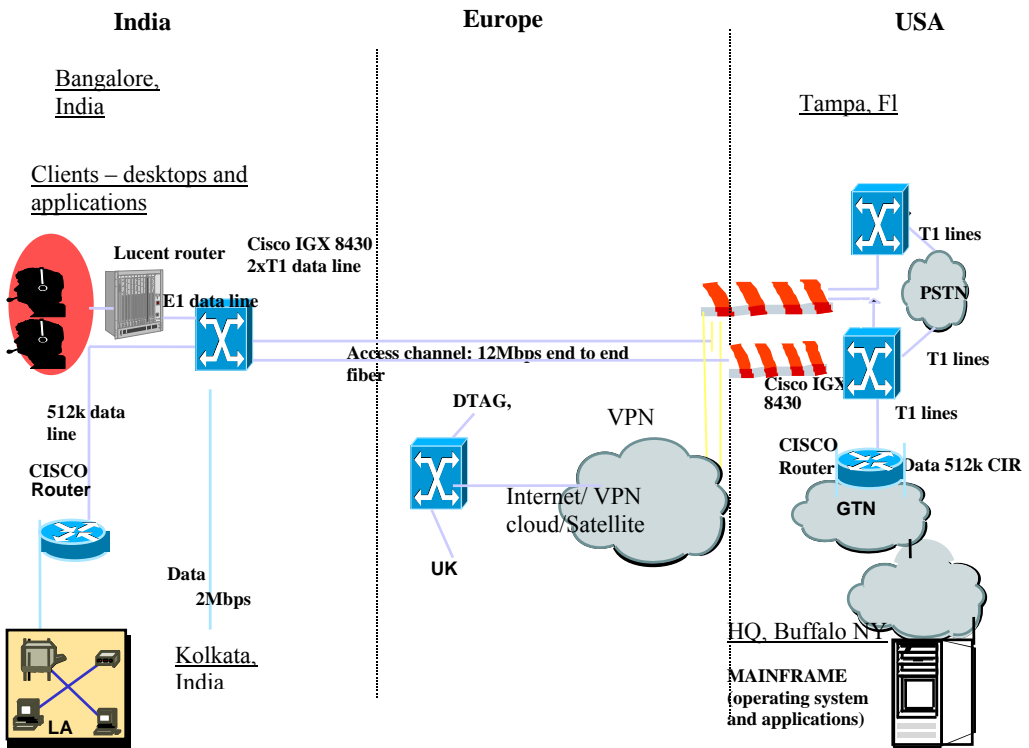


Figure 1: Typical technology infrastructure requirements by off shoring vendors

This infrastructure requires user desktops and applications at the client and server end; routers, PSTN lines and other networking equipment for connectivity. Each of these components creates security concerns that are discussed in the paper.

Classifications of information systems based on vulnerability exposure embody a set of expectations around information classification and controls around the system for security and performance. There are numerous methodologies available for conducting

security assessments, and the decision to utilize a specific method will depend upon the type and complexity of the system, depth of study desired and available resources. The larger and more complex the system, and the more varied its characteristics (including hardware, software, location, function and organizational affiliation), the more difficult it becomes to conduct an effective assessment of the system. Traditional assessment methodologies encompass evaluating the following variables [Freeman, et al. 1997, Sitkin and Pablo 1992]: threats, and their likelihood of occurrence; vulnerabilities, and the degree to which they can be exploited by threats; the harm (consequences) resulting when a security event occurs; the effectiveness of security mechanisms applied to counter the threats.

In such scenarios, a combination of two factors is important: the probability of malfunctioning (failure) and the consequence of malfunctioning (severity). The probability of failure depends on the probability of occurrence of a fault combined with the possibility of exercising that fault. Severity is rated in more than one way and for more than one purpose. For example, the STD-8719.13A, NASA software security standard, defines several types of risks including availability risk, acceptance risk, performance risk, cost risk, schedule risk, etc. The risk is also highly dependent on the supplier's characteristics (size, stability and expertise)[Earl 1996].

Classifying the architectural elements according to their relative importance along dimensions such as severity and complexity helps in identifying components with high risk, which could require more development resources. In large hierarchical systems, a system is composed of several subsystems, which in turn are composed of components and connectors. The system (subsystem) risk is assessed as an aggregate of individual component and connector risk factors. To classify subsystems according to risks, we need to develop algorithms that aggregate risk factors of the constituents to the subsystem level. This enables a comparison of risk factors for subsystems, which guides the process of identifying critical architecture elements and analyzing the effect of replacing components with new ones with improved quality, i.e. lower risk estimates. This is done by studying the sensitivity of the application risk to variations in the risk factors of architecture components and connectors.

2.1 Risk assessment frameworks

Several papers have appeared in the literature that describes “risk assessment” methods. However, none of the papers have researched the end-to-end application of the interactions amongst components and connectors. The most common assessment of risk

involves using a function relating the consequences of undesirable events and their likelihood. But the papers rarely describe how components enter into the equation. As a result, it is not clear what security “risk assessment” entails in global systems. This is one of the gaps in existing literature that our framework attempts to fill.

In this sub-section we review several risk assessment methodologies. One of the most commonly used risk assessment frameworks is *OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)* [Alberts and Dorofee 2002]. This approach concentrates on assets, threats and vulnerabilities. The threat profile of different assets is used to determine the risk decisions. Another frequently cited approach is *the CORAS (Construct a platform for Risk Analysis of Security Critical Systems) methodology* [Stolen, et al. 2002]. The CORAS methodology is based on UML (Unified Modeling Language), a language that uses diagrams to illustrate relationships and dependencies between users and the environment in which they work. In CORAS, the UML class diagrams of each asset are the basis used for decisions. *ISRAM (Information Security Risk Analysis Method)* [Karabacak and Sogukpinar 2005] is another risk assessment framework that uses a quantitative approach that allows for the participation of the manager and staff of the organization. ISRAM is a survey-based model wherein two separate and independent surveys are conducted for the two attributes of risk, namely probability and consequence. Here, again, the focus is on threat or a specific vulnerability. Adding cost as a major factor in risk analysis, *Cost-Of-Risk Analysis (CORA)*[International Security Technology Inc (IST Inc) 2000] risk model uses data collected about threats, functions and assets, and the vulnerabilities of the functions and assets to the threats to calculate the consequences, that is, the losses due to the occurrences of the threats. This is a widely used approach to interweave costs considerations in risk analysis[Lao and Wang 2007].

Prior literature has also identified that application architectures deployed using internet technologies can be segregated into Operating System and Computing Hardware, Network Services, Middleware and Application layers [Agrawal, et al. 2003]. Rather than concentrating on any particular layer in the architecture, in this paper, we analyze a system/architecture independent of the layers, as atomic elements contributing to the overall security threat of the architecture [Bass, et al. 2003, Shaw and Garlan 1996]. We take a holistic approach and embed considerations of vulnerabilities and ensuing threats in the selection of specific security technology.

We distinguish from these approaches in terms of level of analysis. Our unit of analysis includes end-to-end security analysis vis-à-vis specific technologies used to mitigate the risks and not on analysis of threats per se. Commonly, such analysis covers the threat profiles that are implicit in the nature of discussions of various components and access channels. The paper illustrates the dependencies of various components along an access channel and corresponding dependencies are measured in context of a GDW or an outsourcing arrangement. User component is also broadly included, as user based metrics in the framework, to emphasize relevance. Drawing upon many of the concepts in the above methodologies, we develop a risk measure for the system. The uncertainties in component risk factors and their effect on the overall risk of the system are assessed. A Scoring scheme such as a range from 1 to 10 can be assigned to each factor. With an understanding of the types of risks and

information systems exposure and importance to business, the risk manager, the system manager or information security professional can classify the systems. The classification takes into account factors such as business criticality, sensitivity of information accessed by the system, risk exposure, availability and usage volume, as mentioned in Table 1.

Table 1: Classification Factors

Classification Factors
Business Criticality
Information Sensitivity
Risk Exposure
Availability
Usage Volume

3. INTERNET TECHNOLOGY COMPONENTS

The modern approach to the conceptualization and design of large information systems is based on software components. In our discussion, we have emphasized components that provide or pertain to security of information. The association between information and components is based on the information flows through the components. Information System design and development based on architectures shifts the focus towards architecture elements such as components and connectors where connectors are treated as top-level constructs.

Organizational adoption of Internet technologies is relatively simple because the standards used on the World Wide Web are fairly easy to use (e.g., web browsers, HTML) and the cost of developing an Internet presence can be

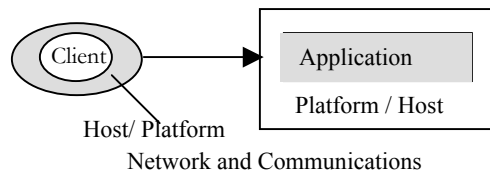


Figure 2: Components

relatively low. Internet technology components are therefore extremely important in the design and implementation of global distributed workplaces. We have classified Internet Technology components in 4 classes based on the component location in typical systems architecture (Figure 2); Client/User Security Components; Application Security Components; Network and Communications Security Components; Host and Platform Security Components.

Although the construction of individual security components has received much attention over the years, very few researchers have examined how components can best be selected for security construction of the overall infrastructure. Discussion of components here is to lay out a concise set of components to provide the risk manager with the security components that would best fit requirements and performance in context of a GDW or an outsourcing arrangement. This Section gives an overview of some of the mechanisms and technologies and discusses them in regard to overall system architecture, location sensitivity and security.

Independent security technologies, such as intrusion detection, firewalls, or virtual private networks, have respective drawbacks and limitations. So, cooperation among various security technologies is necessary. The next section on access channels considers the different physical topologies in conjunction with the set of components discussed in this section in context of a GDW or an outsourcing arrangement.

Though some of the components illustrated in the 4 classifications may be not be security components in the conventional sense, we believe a brief discussion on them is important. For example, we have included routers and switches to emphasize the significance of the functions these devices perform though it can be argued that they are not providing any specialized security function.

The costs associated with information security activities relate to a host of items, including hardware, software, and personnel. We have excluded the cost dimension from the framework to focus primarily on detailed analysis of technology components of security. Also, excluding costs from the discussion enables the risk manager to access all significant variables that would go into any such discourse in light of other external and internal factors most corresponding to the situation.

3.1 Client/user security components

Any software or technology used within a user's context, such as the computer and peripherals could be exposed to security risks. Examples include web browsers, device drivers on the computer and technologies including JavaScript or ActiveX executed on

the machine. Individual components of technology have been extensively studied in terms of evaluating risks and strengths. For example, significant differences can exist amongst different browsers. Felten et al. introduced the term “Web spoofing” and showed how a malicious site could forge many of the browser user interface signals [Felten, et al. 1997]. Tygar and Whitten [Tygar and Whitten 1996] examined both the spoofing potential of hostile Java applets as well as the role of user interfaces in the security of email cryptography systems. Table 2 lists the notations used in the paper and Table 3 presents common components and connectors as they pertain to client and user side security technologies.

Table 2: Notations used in the paper

Symbol	Meaning
CI	Component index, used to tag the components to facilitate later discussions
Γ_a, V_a	Technology component threat index, security index based on architecture components
Γ_c, V_c	Access Channel Threat Index, security index based on access channels
Γ_d	Architecture Distribution Threat index
A_i, A_x, B_i, B_x	Information Systems at locations A and B, where subscript x indicates access over the Internet and subscript i indicates access over Intranet or internal networks
User(x)	A user at Location x.
E_x	A web application hosted by a third party and accessed over Internet.
U_i, C_i, N_i, P_i	User, Application, Network and Platform components
SP_i	Service providers
AC, EAC, SPC	Internal facing, external facing and service-provider components
L_i	Locations
Φ	Overall security assessment of the system
ϕ	Information system classification
γ	Internet technology rating, derived from Γ_a
η	Channel assessment index, derived from Γ_c
λ	User base
ψ	Architecture and component distribution index, derived from Γ_d

Table 3: Client/ user components

Client/User Security Components		
Name	CI	Component Description/ Security Issue Discussion
Browser	U_1	Browsers are potentially, window to users’ systems when used to access web-based resources. Historically, browsers are known for large number of published vulnerabilities. Timely and up-to-date patches is of utmost importance for a secure computing environment.
Cookies	U_2	A cookie is information sent from a web server to a web browser, (usually) stored by the web browser on the client machine for use at a later time. Depending on what information a user has provided to a web server, sensitive data may be in any cookie the web server asks to be stored on that user’s PC.

Java Script	U ₃	Java Script is human-readable program code that can be included on a web page. When a client receives the page, the Java Script code on it runs within the user's browser. Java Script can also run on the server side of a web connection. It can also be used to facilitate a type of attack known as cross-site scripting.
ActiveX	U ₄	ActiveX is a Microsoft technology for downloading miniature executable programs to client machines and then executing them to enhance the user experience of the web site. ActiveX uses a digital certificate (usually signed by a trusted authority like VeriSign) to identify origin of the control.
Signed Applets	U ₅	Signing an applet enables its authenticity and data integrity to be guaranteed by its author, whose identity is verified for by a trusted third party, called a certificate authority.
Storage Media	U ₆	Removable media refers to data storage media that is somewhat portable, that is, it is not permanently fixed to a server or workstation. Different types of removable media include tape, CDR, hard drives, diskettes, flash memory cards and smart cards
Tokens	U ₇	A security token (also known as a hardware token or cryptographic token) is a portable device that a user of is given for authentication. Also can store cryptographic keys and biometric data.
Personal Firewall	U ₈	A personal firewall is traditionally a piece of software installed on an end-user's PC that controls communications to and from the PC and permits or denies communications based on a security policy.

3.2 Application Security Components

The notion of application development using reusable components was first introduced in a 1968 NATO workshop by McIlroy [McIlroy 1968]. A component is a "self-contained entity (blackbox) that exports functionality to its environment and may also import functionality from its environment using well defined and open interfaces" [Emmerich 2002]. Recently, various technologies have evolved to implement re-usable component-based systems to meet increasing demands for distributed computing capabilities have increased. As vulnerabilities get revealed, they may be attributed to different factors including, but not limited to programming errors and the use of less secure technology components. For example, SOAP technologies have made inter-organization communication easier, but since they are transparent to firewalls, they violate an important element of perimeter protection and could expose unforeseen threats.

IT organizations across the globe continually develop, deliver and support complex multi-dimensional systems through a set of virtually connected work enclaves. This information sharing exposes many security concerns in context of a GDW or an outsourcing arrangement. We have listed in Table 4, a number of prevalent Internet component technologies, which are used to enable such information sharing, and the associated security issues. Common attacks on components in Table 4 include remote code execution, SQL injection, format string vulnerabilities, cross site scripting (XSS), buffer overflow, http response splitting, 3rd party misconfiguration, xml & web services

vulnerabilities, hidden field manipulation and username enumeration. These common attacks should be evaluated, for specific component deployment, by the manager assessing the security of these components.

Table 4: Application security components

Application Security Components		
Comp Name	C.I	Component Description/ Security Issue Discussion
Jini	C ₁	Jini is a service-based system running on top of Java, featuring automatic discovery of network services in high performing heterogeneous computing environments. It provides fault tolerance, distributed events, and transaction mechanisms. The inherent Java “sandbox” security model can be mapped onto Jini components, but there are issues related to trustworthiness of the components when allowing external entities incorporated into the internal systems.
Web Services	C ₂	This architecture / set of tools offer integrated, interoperable set of components interacting with each other through a platform-independent mechanism. Typical components for the communication include XML, SOAP, WSDL. Attach security tokens with SOAP messages (X.509) , use XML signature to provide message integrity and message confidentiality with XML encryption. Use PKI model for message identities in handshake of components. The transport layer may be secured using SSL/TLS or IPsec to provide end-to-end security.
CORBA	C ₃	CORBA is a well-known standard providing an architecture for object-based middleware systems. CORBA-based applications are built from distributed objects in different programming languages and reside independently in a heterogeneous networked environment. The interface is defined in a single, language-independent interface description language (IDL) and is accessed by client-side proxies using RPC-based communication protocol. CORBA security service specification of the OMG is based on Trusted Computing Base (TCB) which encapsulates all security-related functionality in a small trusted kernel.
EJB	C ₄	Enterprise JavaBeans (EJB) from Sun Microsystems is a component model for building server-side, enterprise-class applications. The two most important parts in the EJB component model are enterprise beans and the EJB container.
COM+	C ₅	This is an extension over Microsoft’s COM technologies used as a strategic building block for application programs. It adds to COM with an additional set of security layer provisions and operating system services.
.NET	C ₆	This Microsoft framework provides developers with the ability to build and deploy systems over the internet. Communication is achieved using XML queries. The runtime CLR (Common Language Runtime) provides an additional level of security for the .NET framework. The Code Access Security model in the framework also provides administrators ways to properly secure the environment.

3.3 Network and communications Security Components

Deploying on-demand, high availability, converged enterprise networks creates considerable security challenges. The IT community has responded and the results include VPN technologies that incorporate network encryption, access control, and certification and network management. Network and communication security deals with technologies and policies employed to provide security of components that enable

communication among agents of an information system. Enforcement of policies and secure use of technologies provides a secure networking infrastructure. To address the problems of network and communications security, a number of methods can be utilized to formalize network configurations and policies along with tools to ensure configuration integrity. These include types of attack, protocols to protect information at different layers and technologies [49]. Many factors have caused the present status of network insecurity including the Internet's weak support for security, drawbacks & limitations of current security technologies and the dilemma between security performance and cost. An information security manager can adopt complex security policies and technologies to assure the safety of the network, but that usually hurts performance, increase costs, complexity and inconvenience in use. ISPs cope with these new user needs by offering a set of dialup services including remote Internet access as well as secure access to corporate intranets established by means of tunneling protocols like PPP, L2TP and IPSec. Table 5 presents some of the common technologies that enable effective and secure communications infrastructure that and can be used as a starting point to assess security strength of any information system that is globally accessed. Some common security attacks on the components listed include denial of service attacks such as land attack, ping of death, teardrop, fragmentation, UDP storm, syn flood and smurf, TCP hijacking, sniffer attacks, man-in-the-middle attack and eavesdropping.

Table 5: Network and Communications Components

Network and communications Security Components		
Name	CI	Component Description/ Security Issue Discussion
VPN	N ₁	A Virtual Private Network (VPN) allows you to simulate a private network over a public (less secure) network. VPNs are more cost effective because organizations can connect physical locations together without long distance data calls via modem or leasing expensive private communications lines.
RAS	N ₂	RAS, or Remote Access Services, authenticates users connecting to a remote network (via dial-up or the Internet) and allows them access to network resources. If using a standard user/password authentication method, CHAP and MS-CHAP are more secure options than PAP and SPAP. Additional level of security can be added by utilizing the callback feature
Tunneling	N ₃	Tunneling involves encapsulating a protocol within packets carried by a lower-level network. It provides a virtual point-to-point connection. Tunneling can provide a "private" authenticated, encrypted, tamper-resistant connection between two points over the Internet
SSL	N ₄	SSL, or Secure Sockets Layer, is a protocol developed by Netscape for securely transmitting confidential information like credit card numbers across the Internet, between a web browser and web server, by means of public key encryption technology.
TLS	N ₅	Transport Layer Security, is a transport layer protocol based on SSL and is considered to be a more flexible successor to SSL. SSL and TLS use public key encryption, key exchange, and X.509 certificates for communication privacy

		and user/site identification.
HTTP	N ₆	HTTP is the HyperText Transport Protocol used for unencrypted general communications between web browsers and web servers.
HTTPS	N ₇	HTTPS is HTTP with SSL encryption and authentication extensions.
S-HTTP	N ₈	S-HTTP is an alternative to SSL for secure communications between a web browser and web server. It provides similar functionality, but uses different techniques to do so.
IM	N ₉	Instant messaging, or IM, is used to communicate with others on the Internet in near real-time. It is generally a direct peer-to peer, person-to-person communication technology.
P2P) file sharing	N ₁₀	File sharing, by using P2P services such as Kazaa or simple Windows File & Printer Sharing (NetBIOS) connections is an area of concern, because such user-controlled services can be used to make confidential information available to unauthorized people, as well as being a source of (possible) pirated data such as music for which the company could become liable. Peer-to-peer (p2p) File sharing systems are characterized by highly replicated content distributed among nodes with enormous aggregate resources for storage and communication [Kuzmanovic, et al. 2005].
L2TP/ PPTP	N ₁₁	PPTP is an example of a layer 2 protocol that provides encrypted, authenticated tunneling. L2TP is a layer 2 protocol that provides authenticated tunnels, which can be encrypted using the layer 3 IPsec.
SSH	N ₁₂	SSH is often used as a replacement for the telnet terminal communication protocol. Unlike telnet, SSH allows for secure authentication and encrypted communication.
Dial-up / Modem	N ₁₃	Modems directly dialing into your network mean that there are modems waiting for incoming calls on your internal network. Anyone who knows (or finds) the telephone number to these modems can call them and attempt to access your network.
DMZ Topology	N ₁₄	The DMZ, or Demilitarized Zone, on a network is “that portion of a company’s network which sits between the Internet and an internal network’s line of defense, usually some combination of firewalls and bastion hosts”
IDS/ IPS	N ₁₅	An Intrusion Detection System (IDS) is used to detect attempts to break into or misuse a system or network. An IPS has more active response capabilities than IDS, such as shutting down a server on detection of a malicious activity.
SMTP	N ₁₆	SMTP, by default, is not an encrypted protocol. The entire message is transmitted around the Internet in clear text, for all with packet-sniffing software to see.
S/ MIME	N ₁₇	S/MIME, or Secure/MIME, provides sender authentication and message privacy for email. It was developed by RSA Security®, and uses standardized formats for message data and digital certifications. S/MIME is a scalable secure email solution in which the standard hierarchies used in managing
PGP	N ₁₈	PGP, or Pretty Good Privacy, provides the same functionality as S/MIME, but with message data digital certificate formats designed from the ground up, rather than being based on existing standards. PGP provides private, authenticated email communication through the use of public key encryption.
PGP/ MIME	N ₁₉	It is a secure method of sending e-mail that uses the Rivest-Shamir-Adleman encryption system.
WEP/ WAP	N ₂₀	To protect an 802.11b network from unauthorized, use and “snooping”, you can enable packet encryption via WEP. Different cards have different levels of support for WEP. WEP works by using a RC4 encryption scheme, The design in 802.11 for RC4 uses a shared key.
TKIP	N ₂₁	Through TKIP (Temporal Key Integrity Protocol) security you can add to hardware with a firmware upgrade. TKIP is a temporary improvement to WEP security; eventually, it will be replaced by AES just as TKIP is replacing WEP.

WAP/ WTLS	N ₂₂	The Wireless Application Protocol is a wireless technology for wireless resources with limited capability such as a cellular phone. Among the protocols within WAP is the security layer, Wireless Transport Layer Security (WTLS), which provides privacy, data integrity and authentication for WAP communication.
Router s	N ₂₃	A router is a network device that connects networks, forwarding packets to and from them as needed. Routers communicate using special protocols known as “routing protocols. These protocols, like some other Internet protocols, have vulnerabilities, particularly in the area of spoofing.
Switch	N ₂₄	Switches, like routers, forward traffic to the network connections as required. Switches work at a data-link layer, using MAC addresses, rather than at the network layer used by routers.
TACA CS/ TACA CS+	N ₂₅	TACACS is the Terminal Access Controller Access Control System, a client/server user authentication protocol. For authentication, it allows use of user/password information, Kerberos-style authentication that does not require keys being passed over the wire, or even dynamic password systems in which smart cards are used to generate one-time passwords.
FTP	N ₂₆	Vanilla FTP transmits in clear text, exposed to unauthorized disclosure.
S/FTP	N ₂₇	Secure FTP enhances the FTP protocol by allowing it to run over an encrypted connection provided by SSH or SSL, taking advantage of the authentication and encryption features in those protocols.
Tele- com/ PBX	N ₂₈	The same type of vulnerabilities faced by an organization’s data network are also faced by its telephone network, including theft of service (through long distance toll fraud), compromise of data privacy or integrity, unauthorized access to privileged functions, denial of service, and opportunities for reconnaissance by an attacker interested in patterns of calls by one or more users
VLAN s	N ₂₉	A VLAN (virtual LAN) is a logical subnet created by configuring network switches. It provides the benefits of a subnet without requiring the devices on the VLAN be located near each other or connecting using the same physical technology.
NAT	N ₃₀	Network Address Translation (NAT) maps private network addresses to public network addresses, allowing devices on private networks to communicate with outside networks. NAT can be static or dynamic.

3.4 Platform/Host Security Components

Servers host applications and provide interfaces for specialized service delivery such as email, web, DNS etc. The components under discussion include both the services and the operating system platforms they operate on. There are numerous issues with platform and host security in a GDW or an outsourcing arrangement. Most important are the update or patch management processes to control vulnerabilities on the platform. Malicious software such as viruses upgrade constantly, with superior abilities to by-pass detection. Effective and pro-active strategies to manage risks include using appropriate software to carry on security scan, assessment, security deflection detection, and corresponding remedies. Vulnerability scanners can be used to determine the degree of exposure to known vulnerabilities. For example, a popular tool, SATAN (Security Administrator Tool for Analyzing Networks), checks a laundry list of services or conditions that are enabled on a particular machine. Table 6 presents common platform

and host security components that are vital for security considerations and understanding of overall information system in context of a GDW or an outsourcing arrangement.

Table 6: Platform/ Host Components

Platform/Host Security Components		
Name	C.I.	Component Description/ Security Issue Discussion
Anti-virus	P ₁	Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).
OS/NOS hardening	P ₂	Servers are usually a security priority, because they hold valuable resources that need to be accessed by multiple users.
Email servers	P ₃	Email server software is, a fertile ground for software bugs – some of which can be exploited to gain administrative access to the email server. Email servers actually run two different types of protocols. The first type is SMTP (Simple Mail Transfer Protocol) and clients use the second type of protocol, POP3 (Post Office Protocol version 3) and IMAP (Internet Message Application Protocol).
Directory services	P ₄	A directory service is the full-featured electronic version of the white-pages. Information provided by directory services can include sensitive details about the enterprise and its network configuration
Vulnerability Scanners	P ₅	Vulnerability scanners are applications that scan a host or application for identifying vulnerabilities present against a set of signatures of known vulnerabilities.
DHCP Services	P ₆	Dynamic Host Configuration Protocol (DHCP) servers are used to assign and distribute host configuration information to clients who request it.
Patch Management	P ₇	Vendors release updates for various reasons including fixing security issues. Updates for a product (OS or application) are usually available at the vendor’s web site. A patch is a fix to a problem found in software or data. A hotfix is a small patch file, generally targeted to one or two specific issues. Hotfixes are usually developed and released in a short timeframe, with less testing than service packs. A service pack (or update pack) is a collection of patches.
DNS Servers	P ₈	DNS, or the Domain Name Service, is used to map hostnames to IP addresses. In the UNIX world, the most common DNS server is BIND. New protocols such as DNSSEC (DNS Secure) provides for more authentication than the original DNS protocol, and is implemented in BIND 9. To improve DNS security, restrict zone transfers from your primary name server to only your secondary name servers.

3.5. Risk Exposure

For a particular architecture deployment, the risk exposure posed by the individual technology component may be expressed as:

$$V_a = h(X_i), \text{ where } \begin{cases} X \{x: x \in \{U, C, P, N\}\} \\ i = j^{\text{th}} \text{ architecture component} \end{cases} \dots\dots\dots(1)$$

V_a is a mathematical representation of the overall security of the system based on the technology components. The index may be determined by considering the architecture for a particular system in the organization and/or determined for the whole architecture for

.....(2)

the globally distributed organization. The overall threat index for the organization attributed due to the technologies being used may be expressed as:

$$\Gamma_a = f(V_a)$$

Due to the flexibility of the architecture, the value of Γ_a maybe determined at any level of granularity - application, location or across the whole organization. For maximum security in the architecture, the objective would be to minimize the threat level exposure i.e. minimize Γ_a . The threat index Γ_a , will help architects to gauge the threat levels, analyze the likelihood of their occurrences, the elements of the system most vulnerable to each of these threats and hence implement preventive measures to ensure maximum security in context of a GDW or an outsourcing arrangement.

4. INFORMATION ACCESS CHANNELS

As the Internet becomes an increasingly common method to access information systems, its open nature has become a serious problem for security and availability. In this section, we have analyzed the individual links, called access channels in this paper, in the complete access chain from user to information systems. In the previous section we discussed Internet technologies in terms of components and connectors that enable and secure information systems sharing across a global enterprise in context of a GDW or an outsourcing arrangement. In this section, we decompose access channels as analyzable units and determine their interactions with other individual components (Section 3) and the construction of access paths (via access channels).

For a particular architecture deployment, the risk exposure posed by the access channels may be expressed as:

V_c is a mathematical representation of the overall behavior of the system based on the

$$V_c = f(X_i), \quad \left\{ \begin{array}{l} X \{x: x \in \{A, E\}\} \\ i = i^{\text{th}} \text{ access channel} \end{array} \right. \dots\dots\dots(3)$$

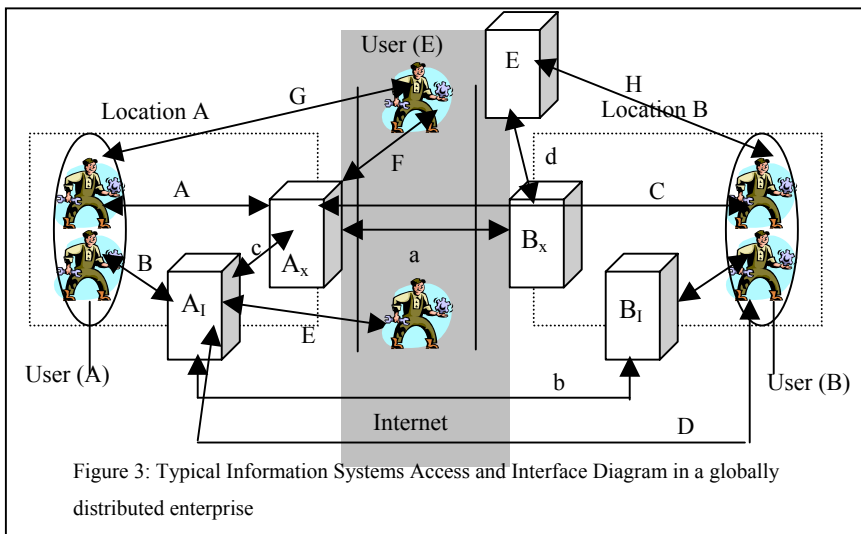
access channels. The index may be determined by considering the open access channels for a particular system in the organization and/or determined for the whole architecture for the globally distributed organization. The overall threat index for the organization attributed due to the access channels being used may be expressed as:

$$\Gamma_c = f(V_c) \dots\dots\dots(4)$$

Due to the flexibility of the architecture, the value of Γ maybe determined at any level of granularity, application, location or across the whole organization. For maximum security

in the architecture, the objective would be to minimize the threat level exposure i.e. minimize Γ_c .

Figure 3 represents a typical information systems distribution, access and interface diagram for a globally distributed enterprise. We have decomposed the mesh of access paths to information systems into 12 access channels (Table 9) that can be individually analyzed for security strength and various access paths can be constructed from them. The communications characteristics as required by the functions of the business and information systems can be categorized into three kinds: System to System (SS); System to User (SU); User to User (UU). Analysis of each kind of communication characteristic



may entail appropriate tools and methods. The diagram represents 2 locations, A and B, of the same global enterprise. An enterprise may have more than 2 locations, but the diagram and ensuing analysis is scalable to n locations without any modifications to the context and flow of analysis presented in this section. Table 7 shows access end points involved in communications to and from information systems.

Table 7: Access End Points

Access End point	Description
A _x	Set of applications hosted for external access at Location A
A _I	Set of applications hosted internally at Location A
B _x	Set of applications hosted for external access at Location B
B _I	Set of applications hosted internally at Location B
E _x	Applications hosted on a third party site and access via Internet.
User (A)	Users at Location A
User (B)	Users at Location B
User (E)	External users accessing applications from Internet

Table 8 shows access channels possible in a globally distributed enterprise. The end points in a channel can be a user or an information system. Channels labeled in upper case (A, B etc.) denote interaction between user and system whereas channels labeled in lowercase (a, ..., d) denote interaction between systems. The third column in the Table 8 represents the type of channel presented in the row. Some channels, such as A and B, are used within a location of the company. This is enabled using internal network with non-routable device addresses (RFC 1918). From Figure 3 and Table 8, we see that there are nine channels that utilize public networks such as the Internet for communication. For example, channel E demonstrates a user, situated outside of company premises, accessing an information system that resides internally within a particular location.

Table 8: Access Channels

Access Channel	End points	Channel Category
A	User (A) – A _x / User (B) – B _x	SU
B	User (A) – A _l / User (B) – B _l	SU
C	User (B) – A _x / User (A) – B _x	SU
D	User (B) – A _l / User (A) – B _l	SU
E	User (E) – A _l / User (E) – B _l	SU
F	User (E) – A _x / User (E) – B _x	SU
G	User (x) – User (y)	UU
H	User (x) – E _x	SU
a	A _x – B _x	SS
b	A _l – B _l	SS
c	A _x – A _l / B _x – B _l	SS
d	A _x – E _x / B _x – E _x	SS

Typically, such a scenario would involve tunneling of communications over Internet for identification and connection with a non-routable address (identifier). This channel is evidently different from C, where the information system interface resides in a DMZ or at a location that is open to direct access over the Internet using a routable Internet address. Use of technologies such as firewall and NAT may be mandated for such channels in context of a GDW or an outsourcing arrangement.

4.1 Channel Access and Internet Technology Components: An Example

Consider the representation of the interaction when a user at Location A accesses an

Table 9: Active/ Passive technology Participation

ATP (Active Technology Participation) = {U ₈ , A ₃ , N ₁ , N ₃ , N ₄ , N ₇ , N ₁₃ }
PTP (Passive Technology Participation) = {U ₁ , U ₇ , U ₈ , N ₂ , N ₁₅ , N ₂₄ , N ₂₅ , P ₁ , P ₂ }

information system located internally within location B [User (A) – BI]. Using this in conjunction with the technologies mentioned in Section 3, we can have 2 baskets of technologies. One basket includes an active set of technologies and the other includes a passive set. Active set of technologies can be directly traced back to user activity at the moment, such as a transaction submission in an application. Passive set of technologies do not change significantly with user actions and include activities such as personal firewall, patch level of user system, etc. The overall security of the information system arising from the interplay amongst components and connectors would be the resultant security from both the baskets. An example would be a user using Internet explorer to access an SSL enabled application that is coded in ASP and has ActiveX and JavaScript components. The communication takes place over Internet using dial-up and VPN, using token-based authentication such as ActiveCard® in context of a GDW or an outsourcing arrangement. The components in the active and passive technology component sets, as presented in table 9, are referred in Table 3 – Table 6.

Table 10: Number of Access Channels

Location	Channels
A _x	A, C, F, a, c and d.
A _I	B, D, E, b and c.
E _v	H and d

An information system can also be accessed by more than one channel. For example, a system hosted for external access, such as A_x at location A, could be accessed by channels A, C, F, a, c and d. We can generalize that given a component distribution of the system and uniform classification rating, a system with fewer open channels will be more secure than a system with more open access channels. Table 10 summarizes the channels possible for any application, based on its three different locations – internal, external and third party. This does not include any user-to-user level communications, which is derived directly from Table 8. Based on a determination of Internet technologies participation baskets (ATP and PTP) from Table 9, we can determine the security strength of the information system, when shared across globally distributed locations.

5. COMPONENT DISTRIBUTION OF INFORMATION SYSTEM ARCHITECTURES

The component distribution framework proposed in this paper looks at the spatial distribution of

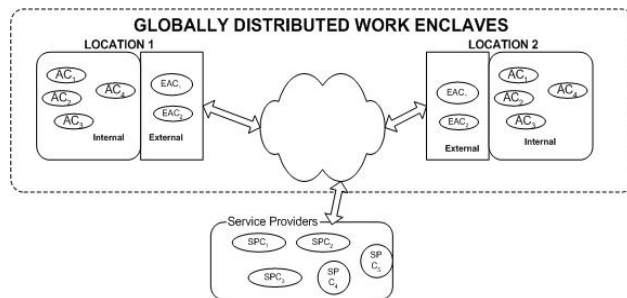


Figure 4: Globally Distributed architectures

components in a globally distributed workplace, where a single organization is operating from two or more distant locations. The collaborative environment provided is transparent to end-user systems, which may be accessed over the Internet in context of a GDW or an outsourcing arrangement. The collaboration dynamics of participants in such a distributed environment leads us to the following component representations:

GDW_i = A globally distributed workplace for an organization

L_i = Any particular geographic location within a particular organization.

SP_i , in turn can be operating within the confines of a different workplace, GDW_j .

Each geographically dispersed entity is segregated into two portions:

Internal: no component within this boundary may interact directly outside the confines of the geographic location.

External: this region faces the “outside” world and serves as the domain where the secured interaction and handshaking of the collaborative environment occurs.

Each entity has components that interact with each other to enable collaborative computing in an outsourcing context. This is indicated by a suffix “C” in Figure 4.

Following the semantics, there are three distinct categories of components:

1. *Internal Facing components*: AC_k : Each L_i has a basket of components which collaborate and are within the boundaries of the geographic location.
2. *External Facing Components*: EAC_i : Components which lie in the “external” facing region of the architecture distribution
3. *Service Provider Components*: SPC_m : Components within this boundary operate outside the confines of a GDW_i , and provide services that enable information sharing over the world-wide-web. It is assumed that the external service provider entity is operating as a single large unit without any geographical dispersion. However, due to the dynamics of the framework, we can generalize the discussion to consider the granular

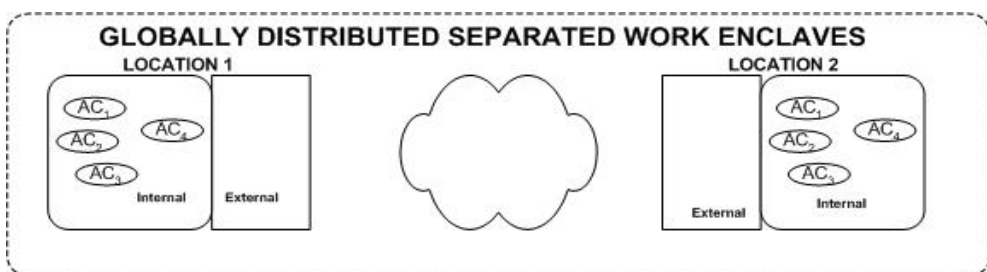


Figure 5: Globally Distributed Workplace – Isolated

distribution of the components within the service provider’s boundaries in context of a GDW or an outsourcing arrangement.

With this framework in place, we can now analyze the dynamics of the organization and develop the following possible scenarios of the architecture distribution. Any system can typically be mapped into one of these scenarios:

1. *Independent Locations, with no external service providers (Figure 5):* There are no external facing components involved in the operating environment. In this scenario, the dispersed locations operate independently with no systemic collaboration involved. All components $AC_1 - AC_n$, lie within internal boundaries. No service providers are involved in this interaction. It also assumes that all components are mirrored internally at any location L_i . This could happen for a number of reasons including, but not limited to, operational limitations by the prevailing local policies, infrastructural limitations, security concerns, organizational dynamics and risk aversion. A typical example would be where the two locations are in two different countries, with different accounting regulations and requiring independent operations in context of a GDW or an outsourcing arrangement.

The scenario may thus be represented as:(5)

$$S_1 = \{x: x \in L_i\}, \text{ where } L_i = \{AC_1, AC_2, AC_3, \dots, AC_n\}$$

Referring back to the access channel assessment in section 4 above, this scenario is representative of access channel B in Table 8. As all the components lie within internal boundaries, the threat level is very low making such architectures much less vulnerable.

2. *Dependent Locations, with no external service providers (Figure 6):* In this scenario, there is systemic collaboration between the geographically dispersed locations. Components exist in both internal and external facing zones of the locations.

$$S_2 = \{x: x \in L_i\}, \text{ where } L_i = \{AC_1, AC_2, AC_3, \dots, AC_n\} \cup \dots \dots \dots (5)$$

$$\{EAC_1, EAC_2, EAC_3, \dots, EAC_n\} \dots \dots \dots (6)$$

As the dispersed locations enable information sharing in this scenario, both entities involve one/more components placed in the external facing zone of the localized

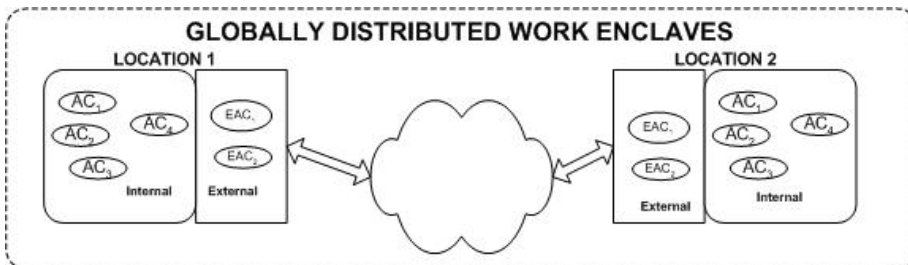


Figure 6: Globally Distributed Workplace – Intra-Organizational Environment

architecture in context of a GDW or an outsourcing arrangement. There is no service provider involvement in this scenario either. Access channels for information sharing would be representative of scenarios C, D described in section 4 above. All these

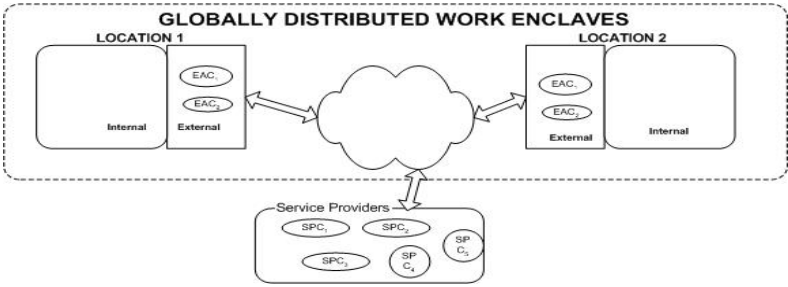


Figure 7: Globally Distributed Workplace – Service

architectures are cumulative and evolving with respect to the access channel for information sharing. Access channels A and B also included in this particular scenario.

3. *Independent Locations, with external service providers (Figure 7)*: This scenario is applicable when an organization conducts its business processes by utilizing only the collaboration provided by service providers. All information sharing enablers in this model exist in the service provider’s domain. This model has enabled many globally distributed organizations stay competitive, create and deliver their products faster, with high quality of service. The stakes for information sharing are very high, as the data exchange operates external to the organization increasing the potential vulnerability of this architecture more so in context of a GDW or an outsourcing arrangement. In order to build an efficient internet-based architecture, this scenario requires components in the external facing zone of the globally dispersed work enclaves.

$$S_3 = \{x: x \in P_i\}, \text{ where} \dots\dots\dots(7)$$

$$P_i = L_i U SP_i, \dots\dots\dots(8)$$

$$L_i = \{EAC_1, EAC_2, EAC_3, \dots, EAC_n\} \dots\dots\dots(9)$$

$$SP_i = \{SPC_1, SPC_2, SPC_3, \dots, SPC_n\}$$

Typical systems in this scenario would be payroll management and document management applications. The access channels representative for this mode of collaborative environment include d, a, F, and C from section 4 above.

4. *Dependent Locations, with external service providers*: Finally, we have the scenario which incorporates all of the above and is probably the most complex architectural distribution for information sharing across a virtual organization. Components are distributed across the internal and external facing zones of the geographically dispersed

enterprise. These components also use services provided by external service providers to enable information sharing over the world-wide-web (Figure 7). This is typical of large, scalable applications brought to a large user base across geographical boundaries in context of a GDW or an outsourcing arrangement. The dynamics of the collaborative environment requires highly complex inter-operational dependencies and appropriate security controls. The scenario may be defined as:

$$S_4 = \{x: x \in Q_i\}, \text{ where} \dots\dots\dots(10)$$

$$Q_i = L_i \cup SP_i \dots\dots\dots(11)$$

$$L_i = \{AC_1, AC_2, AC_3, \dots, AC_n\} \cup \{EAC_1, EAC_2, EAC_3, \dots, EAC_n\} \dots\dots\dots(12)$$

$$SP_i = \{SPC_1, SPC_2, SPC_3, \dots, SPC_n\} \dots\dots\dots(13)$$

The access channels representative for this mode of collaborative environment include all possible modes of information sharing primarily C, D, E, G, a, b, and d, as discussed in section 4.1.

5.1. Component Distribution Threat Index Γ_d

An information systems threat is the danger that information system vulnerability can actually lead to undesirable consequences [Neumann 1995]. Security problems can take place at any stage of the information system life cycle, starting from the architecture blueprint stage until the time when the system is operational. Threats may include but are not limited to fraud, malicious vandalism and natural calamities causing a disruption of service in participating system components. The threat analysis described in this paper can also be an important component in the risk analysis stages of most security design methodologies such as CRAMM (CCTA Risk Analysis and Management Methodology) or BDSS (Bayesian Decision Support System) [Im and Baskerville 2005].

For each scenario, a component distribution index is defined for the overall distribution of components to quantify the risk exposure in context of a GDW or an outsourcing arrangement. Each index is a mathematical representation of the overall behavior of the system based on the characteristics of individual components. The index may be determined by considering the architecture for a particular system in the organization and is determined for the whole architecture of the globally distributed organization. Due to the flexibility of the architecture, the value of Γ_d maybe determined at any level of granularity, application, location or across the whole organization. For any such computation, the value of Γ_d maybe defined as:

$$\Gamma_d = f(S_i) \dots\dots\dots(14)$$

where S_i denotes any combination of the component distribution scenarios described in this section. For maximum security in the architecture, the objective would be to minimize the threat level exposure i.e. minimize Γ_d . Large systems involving multiprocessing, resource sharing, and globalized information sharing have given rise to a new generation of risks due to the increased vulnerabilities of such large scale systems and the potential for fraudulent or malicious misuse of their resources in context of a GDW or an outsourcing arrangement. These risks must be managed since impairment of these large-scale systems, either deliberate or accidental, can have serious consequences for the business in context of a GDW or an outsourcing arrangement. The threat index Γ_d , will help architects to gauge the threat levels, analyze the likelihood of their occurrences, the elements of the system most vulnerable to each of these threats and implement preventive measures to ensure maximum security.

6. THE FRAMEWORK

The paper’s focal contribution is the design and development of a framework to assess the security of information systems used in a globally distributed workplace. This section discusses the framework and describes its relevance as it applies to the system architecture and access method in the context of a GDW or an outsourcing arrangement. The previous sections have described the building blocks used in this stage. The framework can be used by information systems professionals to assess the security level of any information system that is made available for sharing in a globally distributed enterprise. The identification of high-risk components is particularly important for

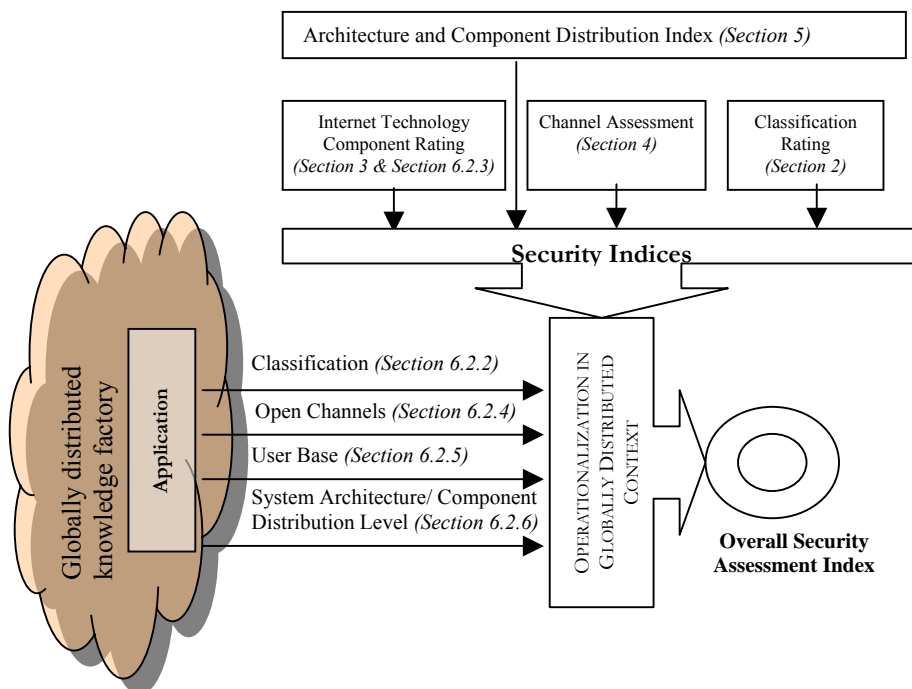


Figure 8: The Security Assessment Framework of an information system enabling

independent verification & validation (IV&V) processes. In our framework, the IV&V resources are focused on these special components, as mentioned in section 3 and 4 to identify possible components that can be identified and assessed at the early stages in a GDW or outsourcing arrangement. Figure 8 presents a visual representation of the framework, showing components, indices and methodology. These applications typically meet organizational objectives such as 24-hour knowledge factories where value creation is achieved through round-the-clock effort and distribution of tasks around the globe, sequentially and progressively. In the following sub-sections, we discuss the variables in the framework and associate them with discussions in the preceding sections. Then, we present a step-by-step methodology to derive a common metric for the security of the information system using two alternate approaches.

6.1 The Variables

The variables of the framework are derived from the previous sections as they pertain to information security assessment in a globally distributed workplace - components and connectors, access channels and architecture and component distribution. The Internet is assumed as the communications and delivery channel.

6.2.1. *Dependent variable*

The dependent variable is the Security Assessment of the information system (Φ).

6.2.2. *Independent variables*

- 1) Information Systems Classification (ϕ)
- 2) Internet Technology Rating (γ)
- 3) Channel Assessment Index (η)
- 4) User Base (λ)
- 5) Architecture and Component Distribution Index(ψ)

$$[\Phi = f(\phi, \gamma, \eta, \lambda, \psi)]$$

The assessment of each of these variables is described in detail in this section.

6.2. The methodology

We have used component analysis to develop the framework by calculating the independent and static complexity of each primitive component and connector. The static complexity at the architecture level is obtained by functions described in the framework by combining the static complexities of primitive parts. Our approach also has similarities with the Failure Mode and Effects Analysis (FMEA) method. FMEA is a systematic approach which, on a component-by-component basis, details all possible failure modes, and identifies their effects on the system [Department of Defense].

We believe that the subjective risk estimations suggested in the framework allow organizations to move quickly to the most important area of risk assessment. In essence, risk assessment is a decision-aid and requires a formal procedure that creates a culture under which situations that can involve risk are constantly sought out [Campbell 1998]. We suggest an ordinal scale for measuring the various indices (eg. severity factor) [Department of Defense 1984]. Table 12 in the following section employs a multi-attribute utility approach for evaluating risk classification of the system[Ahituv 1980]. The utility attributes need to be developed with a focus on definition of the concept behind the attribute, definition of possible measure of the attribute and characterizing the nature of the marginal utility function related to that attribute [Ahituv 1980].

Using utility functions helps us in addressing two important questions that arise owing to the fact that evaluations could potentially be biased [Ahituv 1980]:

- 1) Is the value perceived by the evaluator after assessment of the stakeholders' performance and after the information has been received or is it normative value analytically computed?
- 2) Who is performing the evaluation and when? Is it the decision maker or user, served by the system, who evaluates it either continuously or ex-post; or is it an external or objective evaluator who recognizes all the parameters and performs an ex-ante analysis?

The steps of the framework are as follows:

STEP I. Identification of Information System for security assessment

STEP II. Determination of Information Systems Classification of the System

STEP III. Assessment of Internet Technologies used to derive a common rating from active technology participation and passive technology participation.

STEP IV. Identification and evaluation of access channels and end points to determine channel assessment index

STEP V. Determination of user base accessing the information system.

STEP VI. Evaluation and determination of architecture and component index.

STEP VII. Computation of a security index for the information system.

Details of each step are described below.

6.2.1 Step I

This step involves identification of the information system that is enabled for sharing in a globally distributed enterprise context. The information systems manager would be interested in assessing the strengths of security mechanisms as they pertain to the focal

information system. The framework would provide step-by-step analysis of the various components and channels of the system.

6.2.2. *Step II (ϕ)*

Determine a classification rating for the information system based on discussions in Section 2. Any of the risk assessment methodologies, as mentioned in Sections 1 and 2, can be used to evaluate a classification rating. The scale could be a 10-point scale with 1 reflecting the most important system to protect, and 10 being the least important system. For a large or complex systems, the rank has to be based on a classification of subsystems according to risks. Measures can be developed that aggregate risk factors of the subsystem constituents to the subsystem level. Table 12 in the following section provides critical factors that guide the decision.

6.2.3. *Step III (γ)*

This rating is evaluated based on technologies used in the information systems components. Discussion of different types of technologies, covered in Section 3 can be used to determine an appropriate security rating of the Internet Technology component. This rating will be reflective of both Active and passive technology participations as discussed in Section 3. Γ_a , the Internet technology components index represents a proxy for γ . The methodology discussed in Section 3 and explanations of Γ_a are critical in understanding an appropriate measure of γ .

6.2.4. *Step IV (η)*

This is an index based on assessment of open access channels to an information system. A detailed analysis of procedures and considerations in understanding the factors and methodology to determine an index for channel assessment is presented in Section 4. A subjective evaluation to determine a value from 1 to 10 could be used to determine this index. The discussions around rationale and measure of Γ_c , the channel access index, holds for measurements and methods for η . The methodology discussed in Section 4 and explanations of Γ_c are critical in understanding an appropriate measure of η .

6.2.5. *Step V (λ)*

This variable provides an estimate on the number of users accessing the information system under evaluation. This may be expressed as a comparative ratio representing the proportion of users having access to the information system. An example of implementation would be to normalize the proportion of users in the organization on a

scale of 1-10. For example, if 63% of users have access, it could be represented as $63/10=6$ (rounded).

6.2.6. *Step VI (ψ)*

This is an index for evaluation and assessment of architecture and component distribution of the information system. The index will help managers gauge threat levels, analyze the likelihood of their occurrence, the elements of the system most vulnerable to each of these threats and implement preventive measures to ensure maximum security. The discussions around rationale and measure of Γ_d , the architecture component index illustrates the requirements and instructions for determining a appropriate ψ . The methodology and operational characteristics presented in Section 5 are vital in complete and accurate estimation of ψ .

6.2.7. *Step VII (Φ): Aggregation*

The security posture of an information system can be computed using a mathematical relation amongst the individual security indices. This relation could be a simple addition or a complex function as mandated by the interaction of individual indices amongst themselves. Overall, it can be represented as follows:

$$\Phi = f(\phi, \gamma, \eta, \lambda, \psi) \dots\dots\dots(15)$$

Here Φ represents risk aggregation for the information system that is a roll-up of individual risks to a higher level in the areas of data classification (ϕ), technology rating (γ), channel (η), user base (λ) and component (ψ) assessments. We have adopted the technique that relies on qualitative judgment and to summarize risks in critical risk areas in terms of likelihood and consequence. Within each area and process the individual risks are evaluated against a set of established criteria to determine the aggregate risk rating for the area. Assessment of each of the independent variables should be based on likelihood and consequence of impact. The risks are aggregated in our framework, by combining individual indices as explained in step 7 above.

Our proposed method for security analysis may be compared to other popular methods, some of which are listed in Table 11 and have been introduced earlier in Section 2. All the methods involve creation of a risk assessment team, identification of risks, qualitative and quantitative evaluation of the probability and impacts of each of these risks and in some cases, a prioritization of these risks for the implementation of controls.

Table 11: Popular methods of Information Security analysis

Method	Citation	Risk assessment procedure	Risk aggregation procedure
Octave	[Alberts and Dorofee 2002]	Subjective	None, risks are prioritized for action
NIST Risk Management Guide for Information technology systems	[Stonebumer, et al. 2002]	Qualitative and quantitative	Annual loss expectancy (risk matrix)
SANS Introduction to Information Risk Assessment	[Elky 2006]	Qualitative and quantitative	Annual loss expectancy
Security risk management guide	[Microsoft 2006]	Qualitative and quantitative	Loss expectancy and prioritization

A top-level method used for aggregating risks from individual assessments is the Markowitz variance/covariance framework [Markowitz 1991]. The Markowitz model is a theoretical framework for analysis of risk and return and their inter-relationships using statistical analysis for measurement of risk and is widely used for designing efficient financial portfolios. An alternative robust method for aggregating the risk indices is to use the concept of copulas - functions that join a multivariate probability distribution to a collection of univariate marginal probability functions [48]. However, these methods are known to be overly complicated for practitioners. Instead we utilize a conditional expectation approach discussed below that we believe provides a more convenient implementation method from a practitioner’s perspective.

Conditional expectation is the expected value of a real random variable with respect to a conditional probability distribution [Feller 1950]. CE for purposes of our framework is defined as the expected index computed from multiple assessments of the index, where initial assessment is carried out by assessors based on guidelines and information presented in the framework, followed by introduction of additional information directly relevant to the specific framework index. The consideration of additional information towards adjusting changes to the initial value provides a complete assessment incorporating direct factors (initial) and environmental factors (adjustments). For the initial assessment, under conditions of uncertainty, managers may base their decisions on qualitative aspects of choice alternatives. CE allows them to create meaningful updates of the risk estimation by introducing information about the environmental factors around their initial assessment of the index. One further advantage of the Conditional Expectation approach is that the range of risk indices considered is centered on the expected value of the index as changes to initial assessment are typically incremental.

These conditions will vary from system-to-system and from evaluator-to-evaluator. Most assessments in the framework are contingent on evaluator’s knowledge, risk preferences; and context such as enterprise guidelines, available resources, changing security countermeasures and specific threats under which the assessment is carried out. For example, in risk averse operating environments, evaluators would tend to overestimate the potential risks. CE acknowledges the existence of such factors and incorporates them in calculations.

Let $CE(T)$ denote the Expected value for risk index $T \in (\phi, \gamma, \eta, \lambda, \psi)$, conditional upon relevant additional information I that influences the assessment of T . Such additional information may include changes in legal environments, threat landscapes and technology developments. If this information is represented in terms of the probability of the change, then

$$CE(T_{t+1}) = E(T_{t+1} | T_t, P(I_1) > \alpha_1, P(I_2) > \alpha_2, P(I_3) > \alpha_3, \dots) \dots\dots\dots(16)$$

Where $P(I_1), P(I_2)$ are the probabilities of occurrence of external information 1, 2 and α_1, α_2 are threshold probabilities. Equation 17 shows that the unconditional expectations T_t at stage t are modified to T_{t+1} at stage $t+1$ only when the probability of information exceeds threshold α . The additivity property, for aggregating risks is:

$$\Phi = CE = \sum CE_i (i=1 \dots n) \dots\dots\dots(17)$$

where i is the notation for the different risk indices $(\phi, \gamma, \eta, \lambda, \psi)$. This allows us to allocate back the simulated losses to the individual risks sources in a consistent way.

6.3. A Scenario-based example of the Framework

Having developed the framework in the context of a globally distributed enterprise, we now demonstrate its application in an example system. A set of component interactions is triggered by specific input stimuli [Weidenhaupt, et al. 1998]. An example is presented here to illustrate the contributions of the paper and demonstrate the validity of the framework as utilized for a real world scenario. Some of the data, as evaluated for different metrics, has been modified to mask any inadvertent disclosure. This example is based on a real implementation of a human resource utility application that is being used in a GDW context at a mid-sized financial institution in the US. The details provided here are based on a series of interviews conducted with 6 managers and analysts.

SCENARIO: A pervasive web application is used to track performance, projects, manage salaries, vacation holidays and other administrative activities of employees. Employees (about 25,000) in all locations of the organization access the system on a weekly basis to

manage their salaries and benefits. In light of the functions of this application, it holds special considerations for a globally distributed enterprise.

STEP I. Identification of Information System for security assessment

Information System: Time and Attendance web application (TAS). This application is hosted in various locations in the US where a majority of users also reside. The remaining 15% of its users (contract employees) are in India.

STEP II. Determination of Information Systems Classification (ϕ)

TAS is an application that stores sensitive identifiers for all employees of the company such as Social security number, salary information etc. It is also a web-based application with Internet presence for access from locations that are globally separate from the host location. A summary evaluation matrix of risk factors is presented below to derive the classification for the system. A scoring scheme of 1 - 10 is employed for the risk factors, as suggested in Section 2. A rating of 1 indicates that the factor presents minimal risk and 10 indicate extremely high risk. Guidelines for evaluating classification can be derived from the risk factors as listed in Table 12.

Table 12: Example: Classification Rating

Critical Risk Factor	Prime Decision Drivers	Factor risk rating (1-10)
Business Criticality	Business Continuity	8
Information Classification	Confidentiality	9
Exposure	Availability	8
Service-ability	Availability	7
Unauthorized access	Confidentiality/ Integrity	8
Audit-ability / Coherence	Accountability	7
Fraud Detection/Prevention	Accountability / Integrity	9

A classification score of the system (ϕ) could be derived from factor ratings in Table 12. Here, for illustrative simplicity we have designed function $f()$ to complement the simple mean of individual critical risk factor ratings against a baseline score of 10. This complement is introduced to retain quantitative consistency and to imply that the lower rating indicates greater criticality. *Note* that a lower rating for a risk factor indicates minimal risk, whereas lower rating for the information system classification indicates higher criticality.

$$\phi = f(8,9,8,7,8,7,9) = 10 - \text{mean}(8,9,8,7,8,7,9) \dots\dots\dots(18)$$

$$\phi = 2$$

From equation 17 in Section 6, the classification score (ϕ) could be further analyzed for its impact on the overall risk score for the system (Φ). Equation 17 for this index could be represented as:

$$CE(\phi) = E(\phi_{t+1} | \phi_t, P(I_1) > \alpha_1, P(I_2) > \alpha_2, P(I_3) > \alpha_3, \dots) \dots\dots\dots(19)$$

The initial estimate of the index, as determined by managers after factoring in the various parameters, is 1.6. After the initial assessment, the managers re-assessed the value due to the new change management system deployed and their perceived change in the risk likelihood of an adverse event. The index was updated to 2, an increase of 0.4, based on their understanding that the newer system would initially lead to more errors in change management activities on the system. The updated values for this and other indices (covered in this section) were obtained through discussions with the financial institution’s managers. Authors met with the managers several times and walked them through the framework for security assessment of the GDW system as mentioned above. The indices mentioned in this example are based on actual application of the framework in context of the TAS system. There were a few of pieces of information ($I_1 \dots I_n$) regarding the change management system which caused managers to update the initial index value. One such example brought forth was increased uncertainty of appropriate approval chain for critical changes. In this instance, the threshold value for α was determined assessed at 50% for a 0.4 increase in the index.

STEP III. Assessment of Internet Technologies used to derive a common rating (γ) from active technology participation and passive technology participation. Evaluations at this stage are very objective and factual and, so, application of utility functions would not hold. During such evaluations, references to substantiate the outcomes would be beneficial to keep the biases and errors to a minimum.

We determine specific technologies used that hold special concerns from security and availability standpoints of the company. Using the following notation

- U = set of User/Client components.
- C = set of application components
- N= set of network and communications components
- P = set of platform/ host components

If we have the following component/connector sets:

- U = {U₁, U₂, U₃, U₇, U₉, U₁₀ }
- C = {C₁, C₂ }
- N = {N₆, N₁₀, N₁₄, N₁₅, N₁₆, N₂₄, N₂₅, N₃₁ }
- P = {P₁, P₂, P₆, P_s }

A universal set, COMP, would be a union of components from all the four technology component types.

$$COMP = U \cup C \cup N \cup P$$

$$COMP = \{\{U_1, U_2, U_3, U_7, U_9, U_{10}\} \cup \{C_1, C_2\} \cup \{N_6, N_{10}, N_{14}, N_{15}, N_{16}, N_{24}, N_{25}, N_{31}\} \cup \{P_1, P_2, P_6, P_8\}\}$$

$$COMP = \{U_1, U_2, U_3, U_7, U_9, U_{10}, C_1, C_2, N_6, N_{10}, N_{14}, N_{15}, N_{16}, N_{24}, N_{25}, N_{31}, P_1, P_2, P_6, P_8\}$$

For active technology participation and passive technology participation sets (mutually exclusive), we have:

$$COMP = \{ATP\} \cup \{PTP\}$$

Based on definitions of ATP and PTP (Section 4.1) and determinations made by financial institution's managers, following composition for ATP and PTP were made.

$$ATP = \{U_1, U_2, U_3, C_1, C_2, N_6\}$$

$$PTP = \{U_7, U_9, U_{10}, N_{10}, N_{14}, N_{15}, N_{16}, N_{24}, N_{25}, N_{31}, P_1, P_2, P_6, P_8\}$$

$$\gamma = g (f_1(ATP) op_1 f_2 (PTP)) \dots\dots\dots(20)$$

where $g()$ is a function to determine γ from ATP and PTP, using a mathematical operator op_1 ; $f_1(y)$ and $f_2(z)$ are functions to determine values for ATP index and PTP index respectively. For our example, managers believe that following assignments would apply to the case (options were 1-10): $f_1(ATP) = 5$ and $f_2(PTP) = 2$ (lower numbers indicate better selection and implementation of technologies). Also, for keeping the function accessible and usable by the practitioners, we used op_1 as a simple weighted mean of f_1 and f_2 outcomes. The weights for ATP and PTP were subjectively determined by the managers, based on their understanding of this function, to be 2 and 3 respectively.

$$\gamma = g (5 op_1 2) = 3.2$$

From equation 17, the classification score (γ) could be further analyzed for its impact on the overall risk score for the system (Φ). The equation 17, for this index, could be represented as:

$$CE(\gamma) = E(\gamma_{t+1} | \gamma_t, P(I_1) > \alpha_1, P(I_2) > \alpha_2, P(I_3) > \alpha_3, \dots) \dots\dots\dots(21)$$

Internet Technology component was the trickiest for the managers due to the complexity and scale of assessment. Their initial assessment for the index, γ , was 3.6. However, when they considered other environmental factors beyond the one discussed in the paper they modified the index value to 3.2. This was based on a recent trend report published by a leading trade publication that predicted stronger legal reforms that had been recently enacted will deter many casual attackers. Again, the magnitude of decrease was also not the easiest to come up with. We took the average of the estimates given by different evaluators, where range was 0.3-0.5. For all the managers, the α (determined to be 20%

for all the increases, 0.3 – 0.5) was greater than the threshold value that led them to believe that an update to initial value was necessary.

STEP IV. Identification and evaluation of access channels and end points to determine channel assessment index (η). From Table 13 and the assessment of channels discussed in Section 4, we have the following access channels open for the architecture of the system in the example: A, C, F, a, and c. Following Section 4, we determine an assessment of $\eta = 5$ for this open architecture. Again, lower numbers for η indicate a more secure initial channel design, but its dynamics with other sections can influence the overall index Φ for the framework. Here a multi-attribute utility function can be employed for understanding security of access channels. The likely attributes could be complexity of the channels, disclosed vulnerabilities of specific technologies used, users’ level of information security awareness, differences in infrastructure availability and reliability between US (the parent company) and India (offshore office), etc.

Equation 17 for this index could be represented as:

$$CE(\eta) = E(\eta_{t+1} | \eta_t, P(I_1) > \alpha_1, P(I_2) > \alpha_2, P(I_3) > \alpha_3, \dots) \dots\dots\dots(22)$$

The initial index value, based on guidelines and discussions in the paper, was 5. On considering different conditional factors external to the specifics described in the framework, the managers believed that there would be no to insignificantly little change. Even after a few re-assessments with different unlikely conditions, they opted to stick with the value of 5 for the variable. Here, though additional information was made

Table 13: Example: Evaluation of Access Channels and end points

Access Channel	End points	Channel Category
A	User (A) – A _x / User (B) – B _x	SU
C	User (B) – A _x / User (A) – B _x	SU
F	User (E) – A _x / User (E) – B _x	SU
A	A _x – B _x	SS
C	A _x – A ₁ / B _x – B ₁	SS

available to the managers for consideration, none of them thought any information was significant enough to push the value for α beyond the threshold, so no change was made to the initial index value. Given the improved security around access channels attributable to recent huge investments in technology upgrades, the α was set to 80%. This meant that only significant information with huge potential impact could have updated the initial value of index.

STEP V. Determination of user base (λ) accessing the information system.

The overall user base of the application is estimated as 86% of employees for the globally distributed company. Drawing from guidelines in framework presented in Section 6, we follow:

$$\lambda = N/10 \dots\dots\dots(23)$$

$$\lambda = 86/10 = 9 \text{ (rounded)}$$

Equation 17, that incorporates concepts of likelihood and impact on the assessment of a value for this index, could be represented as:

$$CE(\lambda) = E(\lambda_{t+1} | \lambda_t, P(I_1) > \alpha_1, P(I_2) > \alpha_2, P(I_3) > \alpha_3, \dots) \dots\dots\dots(24)$$

The assessors believed that this was the simplest of the indices. Their initial assessment was a value of 5.2. However, after they considered the high consolidation rate that the industry is experiencing and the relatively stable financials of the company, they believed that an index value of 5.8 would be more appropriate for the purposes of the framework. An increase of 0.6 is an estimate based on their perception that an increase of around 10%, with the additional information, would best reflect their situation.

STEP VI. Architecture and component index (ψ).

Location: the application is hosted in the DMZ of one of the 6 locations of the globally distributed company. The system is hosted at the company head office with access being made from offices located in three different countries, including from India that has the largest (in terms of number of employees) offshore center. Four

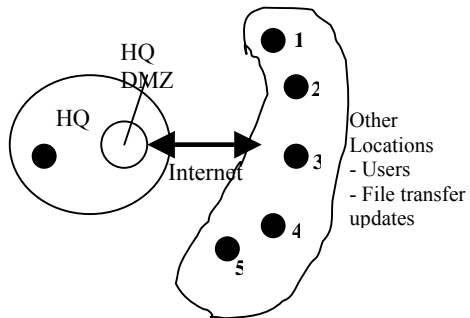


Figure 9: Example: Architecture and Component Distribution

major components of the application sit within the network at headquarters, some in the DMZ and others in the internal network. File upload using FTP happens from all other 5 locations to the FTP server in the DMZ at the head office. (See Figure 9).

From Section 5, we have determined that for this moderately fragmented architecture and component distribution, we have: $\psi = 3$

Equation 17, that incorporates concepts of likelihood and impact on the assessment of a value for this index, could be represented as:

$$CE(\psi) = E(\psi_{t+1} | \psi_t, P(I_1) > \alpha_1, P(I_2) > \alpha_2, P(I_3) > \alpha_3, \dots) \dots\dots\dots(25)$$

Based on information about environmental conditions pertinent to the index ϕ , we can update the index. The initial estimate of the index, as determined by managers after factoring in the various parameters, is 2.4. External information led to an update of the index to 3, where most of the α values for additional information were beyond the threshold. The updated values for this and other indices in this section were obtained through discussions with the institution's managers. α values for 3 different pieces of information were set at 40% (0.3 increase), 30% (0.2 decrease) and 60% (0.5 increase). Since all the α values were met, the resultant change to index ψ was 0.6 (+0.3-0.2+0.5).

STEP VII. Computation of a security index for the information system (Φ).

The overall assessment for the *Time and Attendance* information system would be a function of all the dependent variables as derived in the previous steps. From the framework in Section 6, it could be represented as:

$$\Phi = h(\phi, \gamma, \eta, \lambda, \psi)$$

For our example: $\phi = 2, \gamma = 3.2, \eta = 5, \lambda = 9, \psi = 3$

$$\Phi = h(2, 3.2, 5, 9, 3) \dots\dots\dots(26)$$

h is a mathematical function that can be applied over different variables to compute come Φ . In the first approach, we use simple weighted arithmetic mean, using relative severity and sensitivity of each variable as rated by the assessors. Severity is an important aspect and can be rated in multiple ways for multiple purposes [Kumamoto and Henley 1996]. This is a subjective assignment and will vary based on information system manager's understanding of criticality and requirements of the function variables. The weights used below were agreed upon by the managers through application of the framework (based on their preference and understanding of relative importance of the indices):

$$\phi \rightarrow 2, \gamma \rightarrow 6, \eta \rightarrow 2, \lambda \rightarrow 1, \psi \rightarrow 2$$

$\Phi = [2(2)+6(3.2)+2(5)+1(9)+2(3)] / (2+6+2+1+2)$, yielding 3.71 on a scale of 1 - 10.

Security Assessment Index (<i>weighted average</i>)	$\Phi = 3.71$
--	---------------------------------

As an alternate approach, we can use conditional expectation. The security assessment index Φ for the system can be represented as $CE(\Phi)$, where $CE(\Phi) = \sum CE_i (i=1 \dots n)$.

Using the additive property $CE(\Phi) = [CE(\phi) + CE(\gamma) + CE(\eta) + CE(\lambda) + CE(\psi)] / 5 = [2+ 3.2 + 5 + 5.8 + 3] / 5 = 3.8$

Security Assessment Index (<i>conditional expectation</i>)	$\Phi(CE) = 3.80$
---	-------------------------------------

The two approaches represent the qualitative and objective assessment of the information security system. The managerial implication of this index for information system managers is in terms of exposures to risk threats or vulnerabilities. Both approaches heavily rely on subjective judgments of the evaluators, financial institution’s managers in our case, for determination of different indices as they apply towards the framework. This is also evident from the close scores obtained through the two approaches. However, whereas the weighted average method uses the raw indices, CE uses the updated indices based on environmental information. CE would therefore generally lead to better results owing to the fact that there are more checks for each variable, manifested in the calculation of a central index from two indices that consider likelihood and impact. While the same concepts are also used for the weighted average approach, as managers use similar knowledge to assign weights, functionally application of CE is more formal because CE for individual index explicitly takes into account the manager’s preferences and knowledge in form of adjustments made to the index based on additional information. Lower index denotes that fewer security improvements and investments would be required to reduce the risk exposure to the information system. This means that lower the number, the more secure the information system. A baseline or threshold has to be decided upon by the risk manager to understand relative position of security level of the information and required actions to change the framework index.

6.3.1 Framework Solution Domains

Based on the framework developed in this paper, we can further extend the discussion to help information security strategists in positioning themselves in a particular solution space for an acceptable level of threat. In order to facilitate this mapping, we have plotted

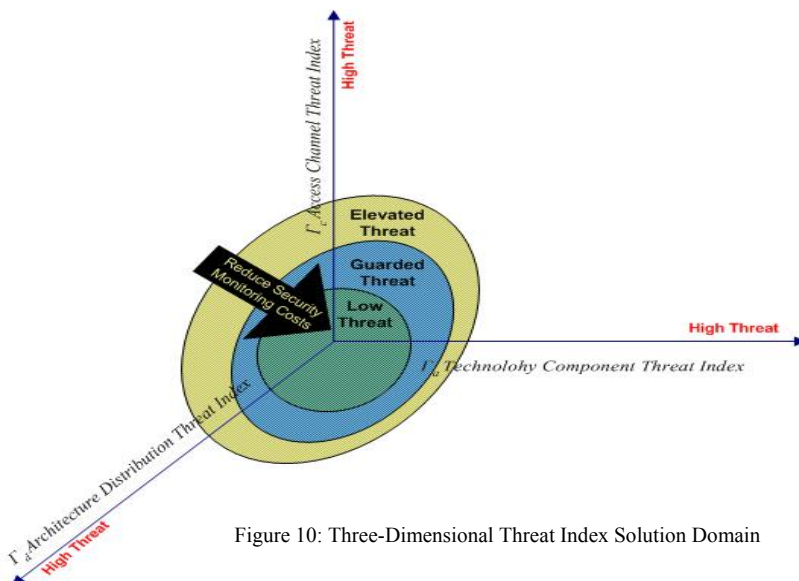


Figure 10: Three-Dimensional Threat Index Solution Domain

the three threat indices derived in the previous sections in this paper along three axes as shown in Figure 10. Along the X-axis, we have plotted the functions described in the sections above: Γ_a (Technology Component Threat Index), the Y-axis has Γ_c (Access Channel Threat Index) while the Z-axis has the Γ_d (Architecture Distribution Threat Index). As these are threat measures, a solution set closer to the origin is more secure.

We have adapted the Color-Coded-Threat Level System formulated by the Homeland Security Advisory System [Security 2006] to define regions on this three-dimensional model to indicate the threat level exposure for any specific architecture/ system in a globally distributed work place. The innermost region is the Low Risk region where the system/architecture is most secure, indicating very low risk for security breaches. Security monitoring costs and threat levels increase with solution sets further away from the origin. Higher costs related to rigorous policy enforcement and implementation of security technologies needs to be examined at regular intervals for the higher threat zones (i.e. Guarded and Elevated). The threat index solution boundaries may be determined through an iterative experimentation within the organization and type of industry. This is also an opportunity for future research to identify optimal solution boundaries for the three-dimensional security domain. This is a subject for future research. The advantages of mapping architecture in a threat solution domain include:

- i) *Ability to position / characterize an existing architecture for a globally distributed work place with respect to threat exposure*
- ii) *Identification of systems which need to be scrutinized for more secure architecture designs and/or allocate more resources for security monitoring*

7. CONCLUSION

Offshore outsourcing allows users of IT Services to benefit from favorable conditions in the offshore location – lower labor costs, ample supply of well-educated labor and quality of service. Services are disaggregated and those service components that need to remain in the US are retained onsite while those that need not be are shipped offshore. For example, in packaged software development, design and marketing stays onsite while coding and customer support are done abroad [Sahajpal, et al. 2006].

One limitation of the paper is the lack of consideration for the risk profiles of the evaluators. For example, if the evaluators are risk adverse, they will be inclined to adopt more risk management mechanisms than might be required. By omitting this consideration, we presumed, when evaluating the metrics for various framework variables, that expected value of assessments could be applied directly, without

considering the evaluators' utility functions. Another limitation is that the costs associated with selecting specific security technologies were not assessed.

Future research may be directed towards a mathematical analysis of the threat exposure levels for each of the four building blocks mentioned in this paper through experimentation and data mining. Future possibilities include determining the security assessment index defined in this paper across a broad set of industries. The framework has wider applicability to risk assessment frameworks even in contexts outside of GDW or outsourcing. Keeping the model presented as base, enhancements could be proposed to introduce more complex calculations for risk evaluations. This should help information security strategists to create threat exposure benchmarks and cost-benefit analysis.

ACKNOWLEDGMENTS

The research of the fourth author was supported in part by NSF under grants 0705292 and 0548917. The usual disclaimer applies. The authors would like to thank the anonymous referees for their critical comments that have greatly improved the paper and also the editors for their encouragement.

REFERENCES

1. AGRAWAL, M., KUO, C.-J., NAM, K. and RAO, H. R. 2003. Electronic Commerce Infrastructure. In Bidgoli, H. ed. *Encyclopedia of Information Systems*, Academic Press, 29-46.
2. AHITUV, N. A Systematic Approach Toward Assessing the Value of an Information System. *MIS Quarterly* 4, 61-75.
3. ALBERTS, C. and DOROFFE, A., 2002. *Managing information security risks, The OCTAVE approach*. Addison Wesley Longman.
4. AXELROD, W. 2007. Analyzing Risks to Determine a New Return on Security Investment. In Rao, H.R., Gupta, M. and Upadhyaya, S. eds. *Managing Information Assurance in Financial Services*, Idea Group, Hershey, PA, 6-36.
5. BASS, L., CLEMENTS, P. and KAZMAN, R., 2003. *Software Architecture in Practice*. Addison Wesley Longman.
6. BROADBENT, M., WEILL, P. and CLAIR, D. S. The implications of information technology infrastructure for business process redesign. *MIS Quarterly* 23, 159-182.
7. CAMPBELL, H. Risk assessment: subjective or objective? *Engineering Science and Education Journal* 7, 57-63.
8. DEPARTMENT OF DEFENSE 1984. Procedures for Performing Failure Mode Effects and Criticality Analysis.
9. DEPARTMENT OF DEFENSE. Procedures of performing a failure mode, effects and criticality analysis.
10. EARL, M. J. The risks of outsourcing IT. *Sloan Management Review* 37, 26-32.
11. EKANAYAKA, Y., CURRIE, W. and SELTSIKAS, P. Delivering enterprise resource planning systems through ASPs. *Journal of Logistics and Information Management* 15, 192- 203.
12. ELKY, S. 2006. An introduction to information system risk management, SANS Institute, 16.
13. EMMERICH, W. 2002. Distributed Component Technologies and Their Software Engineering Implications. In *Proceedings of the Intl. Conference on Software Engineering*, (Orlando, FL), ACM, 537-546.
14. FELLER, W., 1950. *An introduction to probability theory and its applications*. John Wiley and Sons, New York.
15. FELTEN, E. W., BALFANZ, D., DEAN, D. and WALLACH, D. S. 1997. Web spoofing: An internet con game. In *Proceedings of the 20th National Information Systems Security Conference*, (Baltimore, MD).
16. FREEMAN, J. W., DARR, T. C. and NEELY, R. B. 1997. Risk Assessment for Large Heterogeneous Systems. In *Proceedings of the Computer Security Applications Conference*, 44-53.

17. GOKHALE, S. and TRIVEDI, K. S. 2002. Reliability Prediction and Sensitivity Analysis Based on Software Architecture. In *Proceedings of the Intl. Symposium on Software Reliability Engineering (ISSRE 02)*, (Annapolis, MD).
18. GOSEVA-POPSTOJANOVA, K., MATHUR, A. P. and TRIVEDI, K. S. 2001. Comparison of Architecture-Based Software Reliability Models. In *Proceedings of the 12th IEEE International Symposium on Software Reliability Engineering (ISSRE 2001)*, (Hong Kong).
19. GOSEVA-POPSTOJANOVA, K. and TRIVEDI, K. S. Architecture Based Approach to Reliability Assessment of Software Systems. *Performance Evaluation* 45.
20. GUPTA, M., RAO, H. R. and UPADHYAYA, S. Electronic Banking and Information Assurance Issues: Survey and Synthesis. *Journal of Organizational and End User Computing* 16, 1-21.
21. HAGEL III, J. and BROWN, J. S. Your next IT strategy. *Harvard Business Review* 2001, 105-113.
22. IM, G. P. and BASKERVILLE, R. L. A longitudinal study of information system threat categories: the enduring problem of human error. *ACM SIGMIS DATABASE* 36, 68-79.
23. INTERNATIONAL SECURITY TECHNOLOGY INC (IST INC) 2000. Managing risks using CORA.
24. JARVENPAA, S. and LEIDNER, D. Communication and trust in global virtual teams. *Organization Science* 10, 791-815.
25. KARABACAK, B. and SOGUKPINAR, I. ISRAM: information security risk analysis method. *Computers & Security* 24, 147-159.
26. KUMAMOTO, H. and HENLEY, E., 1996. *Probabilistic Risk Assessment for Engineers and Scientists*. IEEE.
27. KUZMANOVIC, A., DUMITRIU, D., KNIGHTLY, E., STOICA, I. and ZWAENEPOEL, W. 2005. Denial-of-Service Resilience in Peer-to-Peer File Sharing Systems. In *Proceedings of the ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*.
28. LAO, G. and WANG, L. 2007. Security Risk Management Strategy of Financial Services Institutions. In Rao, H.R., Gupta, M. and Upadhyaya, S. eds. *Managing Information Assurance in Financial Services*, Idea Group, Hershey, PA.
29. MARKOWITZ, H. M., 1991. *Portfolio selection: Efficient diversification of investments*. Blackwell.
30. MCILROY, M. D. 1968. Mass-produced software components. In *Proceedings of the 1968 North Atlantic Treaty Organisation (NATO) Conference on Software Engineering*, (Garmisch-Partenkirchen), NATO Science Committee, 138 -- 150.
31. MICROSOFT 2006. Security risk management guide, Redmond, WA.
32. NEUMANN, P. G., 1995. *Computer-Related Risks*. ACM.
33. PAWLOWSKI, S., ROBEY, D., AND RAVEN, A. 2000. Supporting shared information systems: Boundary objects, communities, and brokering. In *Proceedings of the 21st International Conference on Information Systems (ICIS)*, (Brisbane, Australia), 329-338.
34. SAHAJPAL, G., AGRAWAL, M., KISHORE, R. and RAO, H. R. 2006. Business Process Offshoring to India: An Overview. In Heinzl, A., Dibbern, J. and Hirschheim, R. eds. *Outsourcing*.
35. SECURITY, D. O. H. 2006. Homeland Security Advisory System.
36. SESHASAI, S., MALTER, A. J. and GUPTA, A. 2006. The Use of Information Systems in Collocated and Distributed Teams: A Test of the 24-Hour Knowledge Factory. In *Proceedings of the SSRN eLibrary*, SSRN.
37. SHARMA, V. S. and TRIVEDI, K. S. 2005. Architecture Based Analysis of Performance, Reliability and Security of Software Systems. In *Proceedings of the 5th ACM International Workshop on Software and Performance (WOSP)*, (Palma de Mallorca, Spain).
38. SHAW, M. and GARLAN, D., 1996. *Software Architecture: Perspectives on an Emerging Discipline*. Prentice-Hall, Upper Saddle River, NJ.
39. SITKIN, S. B. and PABLO, A. L. Reconceptualizing the determinants of risk behavior. *Academy of Management Review* 17, 9-38.
40. STOLEN, K., BRABER, D., F. L. and AAGEDAL, J. 2002. Model-based risk assessment - The CORAS approach.
41. STONEBURNER, G., GOGUEN, A. and FERINGA, A. 2002. Risk management guide for information technology systems, National Institute for Standards and Technology, Gaithersburg, MD, 55.
42. TANNA, G., GUPTA, M., RAO, H. R. and UPADHYAYA, S. Information Assurance metric development framework for electronic bill presentation and payment systems using transaction and workflow analysis. *Decision Support Systems* 41, 242-261.
43. TYGAR, J. D. and WHITTEN, A. 1996. WWW Electronic Commerce and Java Trojan Horses. In *Proceedings of the Second USENIX Workshop on Electronic Commerce*.
44. WEIDENHAUPT, K., POHL, K., JARKE, M. and HAUMER, P. Scenarios in System Development: Current Practice. *IEEE Software* 1998, 34-45.