Computer Systems Security Foundations

Week 2: Security Assessment

<name>

[Pick the date]

This document contains information and typical analyses that Real-Time Integration Systems must conduct to ensure compliance with recent initial public offering (IPO) requirements and to ensure the security of the company infrastructure. In addition to ensuring compliance to the Sarbanes-Oxley requirements, the company is also considering expanding the network infrastructure to allow employee flexibility (yet sound security) in the area of network connectivity through the introduction of a wireless network. The company will evaluate the risks and the current and future network infrastructure and enterprise systems, as well as the access control policies currently in use. Within the analysis of the technical review, Real-Time Integration Systems will ensure a proper security program is in place and that policies and procedures are updated and accurate.

Table of Contents

Project Outline and Requirements (Week 1)

Organization Description

Real-Time Integration Systems is a publicly traded company based in San Jose, California that offers customized solutions to customers and clients. The main focus for Real-Time is the creation of solutions based on integrating the various systems that are used in the customers' offices so that they can have a single management interface for all systems and applications. Real-Time has 100 employees. About one third is internal company-based support, and two thirds of the employee base is consulting staff working on the customized solutions. The company recently underwent an IPO, and as such, now has additional regulatory requirements that it must meet. Talking with the company's chief information officer (CIO) and chief financial officer (CFO), they admit that the recent IPO has added additional pressures for their company. They now must meet additional regulatory requirements.

The consulting staff typically meets with the customer to gather the system requirements and then returns home to the Real-Time facilities to create the integration solutions. A major problem that the consultants face is network resources. The office spaces that are allocated to the consulting team offer cubicles with limited network access. The consultants need a more flexible solution for connecting to the Real-Time network. Real-Time wants to implement a secure solution that ensures the privacy of the communications and company data as well as giving the consultants the flexibility to connect to the network and move around and interact and conference with other consultants.

Project Requirements

As Real-Time starts the project, the leaders realize that their current infrastructure is not as secure as they thought. The original information technology (IT) staff was well-meaning, but at the time of the start-up, they were not as security-conscious as companies are today. As a result, Real-Time wants to ensure the overall security of the existing infrastructure and to isolate the new development infrastructure as much as possible. To begin, the existing network architecture includes a demilitarized zone (DMZ) for the company Web site, file transfer protocol (FTP), and mail servers. The company Intranet is a flat network. All company resources and applications are on the same network with all staff desktops. All company systems are internal (meaning that they outsource no solutions). All systems and applications are housed in the San Jose corporate site in a converted conference room that is now a dedicated data center.

Real-Time does have a concern over the customer systems and data that are brought into the San Jose facility. The customer data and equipment need to be isolated from other customer environments. At no point in time can the data from one customer be stored in the same environment as a different customer. The CIO has made these requirements very clear to the staff. Customer data privacy and security needs to be a top priority.

Proper resources have been allocated for the project, and several key goals have been set:

- Evaluate the regulatory requirements based on the Sarbanes-Oxley Act, and ensure that company security policies are sufficient to meet the requirements.
- Evaluate the security risks in the current environment.
- Evaluate the access control methods that are currently in use, and identify newly needed controls.
- Evaluate the need for controls to better protect data both at rest and in motion.
- Develop or redesign a secure network solution.

Introduction to Information Security (Week 1)

A review of the current infrastructure and security model is needed to ensure compliance with the new Sarbanes-Oxley regulations. Management wants to understand how the regulation impacts the information security posture of the Real-Time Integrations Systems environment. To do so, the following areas need to be better understood by the organization:

- Describe the need for information security
- The potential issues and risks that exist and what benefits they can gain from the new wireless fidelity (W-Fi) project
- Describe what new challenges exist with the new project to allow consultants to work on-site
- Describe the challenges that now apply to the company with the recent IPO taking place

The Need for Information Security

A review of the high level of information security should take place, and then a practical discussion about what it means for organizations like Real-Time Integration Systems needs to take place.

Potential Issues and Risks for Wi-Fi Environments

A review of the technical security needs to take place. The focus should be on the extension of a network through the use of wireless technologies.

Security Challenges of Allowing Consultants to Work On-Site

A review of the administrative security controls needs to take place. The focus should be on the policies and personal requirements that need to be implemented

A Review of the Sarbanes-Oxley Requirements

Sarbanes-Oxley will now affect Real-Time, and there needs to be a discussion about the specific provisions of the regulations that apply to the IT infrastructure.

Security Assessment (Week 2)

To conduct a security assessment, the organization needs to understand its environment. This includes asset identification, data classifications, and network topologies. This section will focus on asset identification and network topology and the risks associated with them in the current environments.

Current Assets

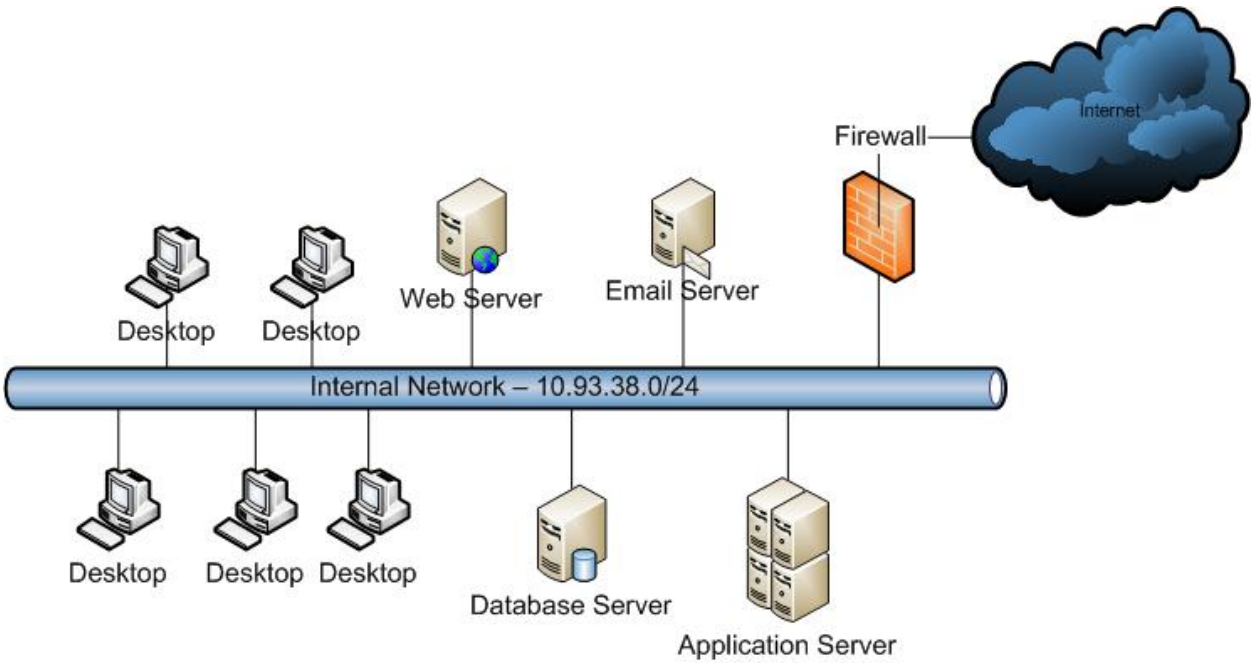
A list of the enterprise systems that Real-Time Integration Systems relies on to run the day-to-day business activities includes the following systems:

Example Enterprise Systems

System	Applications	Description
Enterprise resource planning (ERP)	Human resources (HR)	Human resources uses this to track employees, managers, assignments, salary, and expenses
ERP	Financials	Accounts payables, accounts receivables, general ledger
Customer relations management (CRM)	Sales and marketing	Tracking of customers and customer projects
Web servers	Company public portal	Information and applications used by customers to interact with Real-Time Integration Systems
E-mail server	All departments	E-mail system used for company e-mail and external communications

Analysis of Current Network Topology and Risks

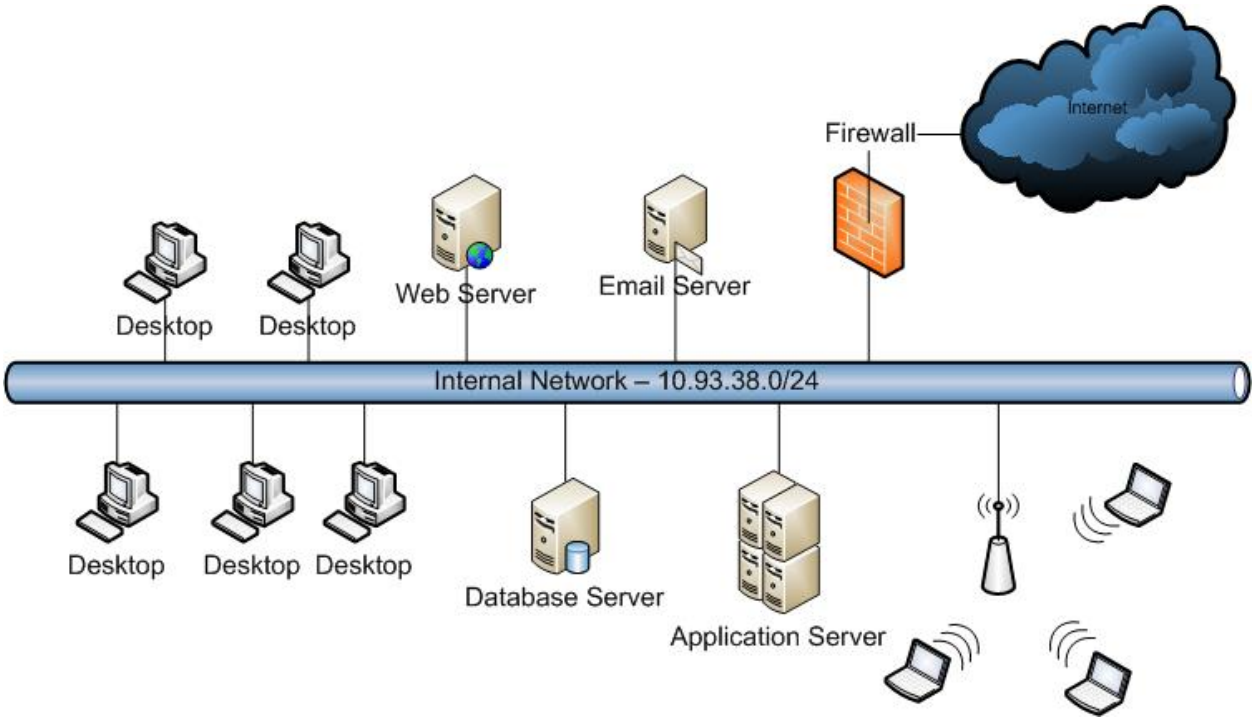
An example diagram for the current network (although not required for submission) could be represented as follows:



Because all machines (user desktops and servers) are on the same network, all connected to the Internet, a security breach on any single machine give hackers direct access to all other servers and devices on the same network. This is highly undesirable. Additional risks should be discussed.

System	Risks
Web server	Accessible to the Internet by design, easy targets for hackers
Desktop systems	Users are primary targets for social engineers, if compromised network resources are accessible

If the new Wi-Fi network is added to the existing network, an example diagram could look as follows:



A discussion about the new risks for this model needs to be conducted.

Risk Assessment Methodology

The following is an outline of the methodology that can be used for a risk assessment:

- **Phase 1:** Project Definition
- **Phase 2:** Project Preparation
    - Team Preparation
    - Project Preparation
- **Phase 3:** Data Gathering
    - Administrative
    - Technical

    - Physical
- **Phase 4:** Risk Analysis
    - Assets
    - Threat Agents and Threats
    - Vulnerabilities
- **Phase 5:** Risk Mitigation
    - Safeguards
    - Residual Security Risk
- **Phase 6:** Risk Reporting and Resolution
    - Risk Recommendation
    - Documentation

Risk Mitigation

As part of the risk-assessment process, a plan needs to be recommended (and ultimately acted upon). The exact process for dealing with risk varies from company to company based on the risk tolerance. The following should be discussed with respect to handling risk:

- Transfer
- Avoid
- Reduce
- Accept

Access Controls and Security Mechanisms (Week 3 TBD)

Software and Database Security (Week 4 TBD)

Network Security (Week 5 TBD)

References