GLOBAL FINANCE, INC. (GFI)

Global Finance, Inc. (GFI) is a financial company that manages thousands of accounts across Canada, the United States, and Mexico. A public company traded on the NYSE, GFI specializes in financial management, loan application approval, wholesale loan processing, and investment of money management for their customers.

GFI employs over 1,600 employees and has been experiencing consistent growth keeping pace with S&P averages (approximately 8%) for nearly six years. A well-honed management strategy built on scaling operational performance through automation and technological innovation has propelled the company into the big leagues; GFI was only recently profiled in Fortune Magazine.

The executive management team of GFI:

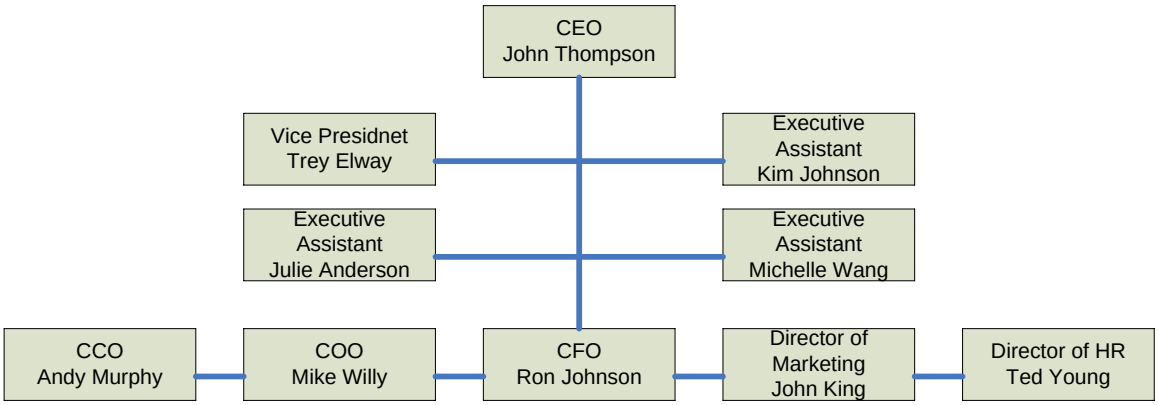


Figure 1 GFI Management Organizational Chart

BACKGROUND AND YOUR ROLE

You are the Computer Security Manager educated, trained, and hired to protect the physical and operational security of GFI's corporate information system.

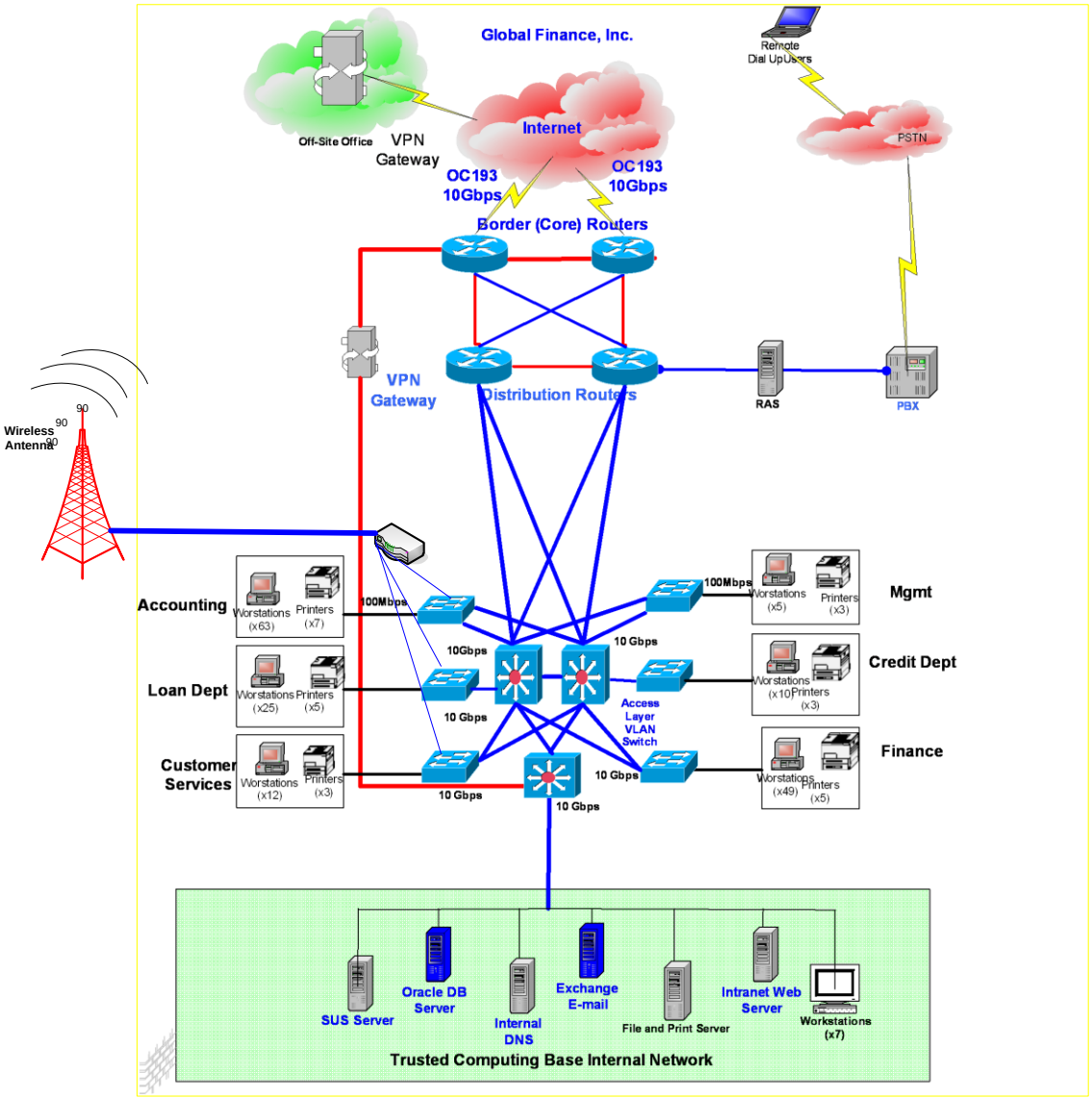
You were hired by COO Mike Willy and currently report to the COO. You are responsible for a $5.25m annual budget, a staff of 11, and a sprawling and expansive data center located on the 5th floor of the corporate tower. This position is the pinnacle of your career – you are counting on your performance here to pave the way into a more strategic leadership position in IT, filling a vacancy that you feel is so significantly lacking from the executive team.

There is actually a reason for this. CEO John Thompson believes that the IT problem is a known quantity – that is, she feels the IT function can be nearly entirely outsourced at fractions of the cost associated with creating and maintaining an established internal IT department; the CEO's strategy has been to prevent IT from becoming a core competency since so many services can be obtained from 3rd parties. Since the CEO has taken the reigns two years ago, the CEO has made significant headway in cutting your department's budget by 30% and reducing half of your staff through outsourcing. This has been a political fight for you: maintaining and reinforcing the relevance of an internal IT department is a constant struggle. COO Willy's act of hiring you was, in fact, an act of desperation: the increasing operational dependence on technology combined with a diminishing IT footprint gravely concerned Jacobson, and he begged to at least bring in a manager to whom these obligations could be delegated to. Jacobson's worst nightmare is a situation where the Confidentiality, Integrity, and Availability of the information system was compromised – bringing the company to its knees – then having to rely on vendors to pull him out of the mess.

GFI has experienced several cyber-attacks from outsiders over the past a few years. In 2012, the Oracle database server was attacked and its customer database lost its confidentiality, integrity, and availability for several days. Although the company restored the Oracle database server back online, its lost confidentiality damaged the company reputations. GFI ended up paying its customers a large sum of settlement for their loss of data confidentiality. Another security attack was carried out by a malicious virus that infected the entire network for several days. While infected the Oracle and e-mail servers had to be shut down to quarantine these servers. In the meantime, the company lost $1.700, 000 in revenue and intangible customer confidence.

There's no question that the company's CEO sees the strategic importance of technology in executing her business plan, and in this way you share a common basis of principle with her: that IT is a competitive differentiator. However, you believe that diminishing internal IT services risks security and strategic capability, whereas the CEO feels she can acquire that capability immediately and on the cheap through the open market. You're told that CEO Thompson reluctantly agreed to your position if only to pacify COO Willy's concerns.

CORPORATE OFFICE NETWORK TOPOLOGY



You are responsible for a corporate WAN spanning 10 remote facilities and interconnecting those facilities to the central data processing environment. Data is transmitted from a remote site through a VPN appliance situated in the border layer of the routing topology; the remote VPN connects to the internal Oracle database to update the customer data tables. Data transaction from the remote access to the corporate internal databases is not encrypted.

A bulk of the data processing for your company is handled by Oracle database on a high end super computer. The trusted computing based (TCB) internal network is situated in a physically separated subnet. This is where all corporate data processing is completed and internal support team has its own intranet web server, a SUS server, an internal DNS, an e-mail system, and other support personnel workstations. Each corporate department is segregated physically on a different subnet and shares the corporate data in the TCB network.

OTHER CONSIDERATIONS

1. Ever since the article ran in Fortune about GFI, your network engineers report that they've noted a significant spike in network traffic crossing into the internal networks. They report that they cannot be certain what or who is generating this traffic, but the volume and frequency of traffic is certainly abnormal. The management is very concerned over securing the corporate confidential data and customer information.

2. Increasingly, GFI's CEO Thompson attempts to outsource IT competency. In fact, you've been told of a plan from COO Willy to outsource network management and security functions away from your department and to a service integrator. COO Willy warns you that the political environment will only become more contentious over time; you must make a compelling case as to what value your department can bring over an integrator that can provide secure services at 40% less annual cost than you.

3. The interrelationship between data and operations concerns you. Increasingly, some of the 10 remote sites have been reporting significant problems with network latency, slow performance, and application time-outs against the Oracle database. The company's business model is driving higher and higher demand for data, but your capability to respond to these problems are drastically limited.

4. Mobility is important for the organization to interact with the customers and other co-workers in near real-time. However, the CEO is concerned with the mobility security and would like to research for the best practice for mobility computing. The CEO is willing to implement a BYOD policy if security can be addressed.

5. Employees enjoy the flexibility of getting access to the corporate network using a WiFi network. However, the CEO is concerns over the security ramifications over the wireless network that is widely open to the company and nearby residents.

6. The company plans to offer its products and services online and requested its IT department to design a Cloud Computing based e-commerce platform. However, the CEO is particularly concerned over the cloud computing security in case the customer database is breached.

ASSIGNMENTS

- Identify and describe the organizational authentication technology and network security issues.
- Make a list of access points internal and external (remote).
- Design a secure authentication technology and network security for GFI.
- Make assumptions for any unknown facts.
- List all known vulnerabilities you can identify in this environment and address them by proposing a new design. You may use any combination of technologies to harden authentication process and network security measures.
- Address the CEO's concern over the mobility security and design a secure mobile computing (smart phones, tablets, laptops, etc.) in terms of authentication technologies and data protection.
- Identify wireless vulnerabilities and recommend what safeguards, authentication technologies, and network security to protect data should be implemented.
- Design a cloud computing environment for the company with a secure means of data protection at rest, in motion and in process.

Risk Assessment Paper Rubric

You are given a fictional scenario above describing security issues affecting organizational assets. You will identify the risks associated with the assets, and recommend mitigating procedures. You will prepare a **quantitative** / **qualitative** risk assessment to address risk factors on organizational assets. Your final paper will be 15–25 pages long in a Word document and will be graded using the following rubric.

Criteria	Non-compliant	Minimal	Compliant	Advanced
Inventory assets and prioritize them in the order of mission criticality.	Did not inventory or prioritize assets in the order of mission criticality. (1)	Inventoried assets but did not prioritize them in the order of mission criticality. (3)	Inventoried, prioritized assets, but did not address mission objectives in their asset priority. (6)	Inventoried, prioritized assets and addressed mission objectives in their asset priority. (10)
Evaluate enterprise topology and perimeter protection.	Did not evaluate enterprise topology and perimeter protection. (1)	Evaluated enterprise topology but did not include perimeter protection measures. (3)	Evaluated enterprise topology, perimeter protection measures, but did not address mission objectives. (6)	Evaluated enterprise topology, perimeter protection measures, and addressed mission objectives. . (10)
Evaluate remote access to the networks.	Did not evaluate remote access protocols and safeguards to the network. (1)	Evaluated remote access protocols but did not address security safeguards to the network. (3)	Evaluated remote access protocols, security safeguards to the network, but did not address mission objectives. (6)	Evaluated remote access protocols, security safeguards to the network, and addressed mission objectives. (10)
Evaluate authentication protocols and methodologies.	Did not evaluate authentication protocols and methodologies. (1)	Evaluated authentication protocols, methodologies but with insufficient data or inadequate description. (3)	Evaluated authentication protocols, methodologies with supporting data and description, but lacks mission objectives. (6)	Evaluated authentication protocols, methodologies with supporting data, description; and addressed mission objectives. (10)
Assign asset values to organization assets for quantitative / qualitative risk assessment.	Did not assign asset values to organization assets for quantitative / qualitative risk assessment. (1)	Assigned asset values to organization assets for quantitative / qualitative risk assessment but incomplete. (3)	Assigned asset values to organization assets in a complete inventory, but did not address mission objectives. (6)	Assigned asset values to organization assets in a complete inventory, and addressed mission objectives. (10)
Assess vulnerabilities on each asset and impacts if compromised.	Did not assess vulnerabilities on each asset and impacts if compromised. (1)	Assessed vulnerabilities on each asset and impacts if compromised; but incomplete. (3)	Assessed vulnerabilities on each asset and impacts if compromised; of complete inventory but did not address mission objectives. (6)	Assessed vulnerabilities on each asset and impacts if compromised; of complete inventory and addressed mission objectives. (10)
Assess risk based on probability of compromise and its impact discovered on each asset.	Did not assess risk based on probability of compromise and its impact discovered on each asset. (1)	Assessed risk based on probability and its impact discovered on each asset but incomplete. (3)	Assessed risk based on probability and its impact discovered on each asset but did not summarize them. (6)	Assessed risk based on probability and its impact discovered on each asset and summarized them. (10)

Criteria	Non-compliant	Minimal	Compliant	Advanced
Recommend risk mitigation procedures commensurate with asset values.	Did not recommended risk mitigation procedures commensurate with asset values. (1)	Recommended risk mitigation procedures commensurate with asset values, but incomplete. (3)	Recommended risk mitigation procedures commensurate with asset values of complete inventory, but did not address mission objectives. (6)	Recommended risk mitigation procedures commensurate with asset values of complete inventory, and addressed mission objectives. (10)
Formulate 15-25 pages of a quantitative or qualitative risk assessment in APA format.	Did not follow proper quantitative or qualitative risk assessment format, and failed to conform to APA format. (1)	Followed proper quantitative or qualitative risk assessment format but did not conform to APA format. (3)	Followed proper quantitative or qualitative risk assessment format and conformed to APA but insufficient reference list and page count. (6)	Followed proper quantitative or qualitative risk assessment format and conformed to APA in a sufficient reference list and page count. (10)
Executive summary of risk assessment.	Did not include an executive summary. (1)	Included an executive summary but lacks details. (3)	Included an executive summary in details, but did not address the mission objectives. (6)	Included an executive summary in details, and addressed mission objectives. (10)