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.

The diagram below displays the executive management team of GFI:

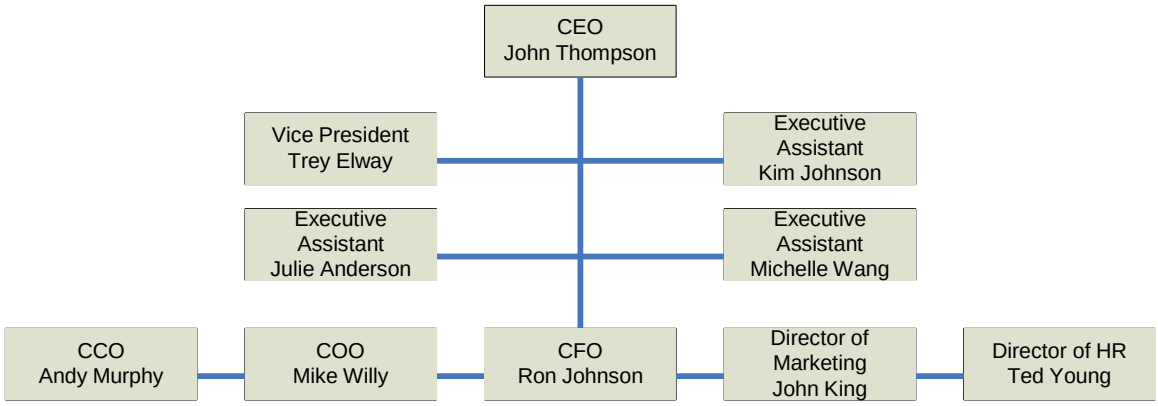


Figure 1 GFI Executive Organizational Chart

BACKGROUND AND YOUR ROLE

You are the Chief Security Officer, hired by COO Mike Willy, to protect the physical and operational security of GFI's corporate information systems. Shortly after starting in your new position, you recognize numerous challenges that you will be facing in this pursuit.

Your primary challenge, as is usually the case, is less technical and more of a political nature. CEO John Thompson has been swept up in the "everything can be solved by outsourcing" movement. He believes that the IT problem is a known quantity and feels the IT function can be almost entirely outsourced at fractions of the cost associated with creating and maintaining an established internal IT department. In fact, the CEO's strategy has been to prevent IT from becoming a core competency since so many services can be obtained from 3rd parties. Based on this vision, the CEO has already begun downsizing the IT department and recently presented a proposal to his senior management team outlining his plan to greatly reduce the internal IT staff in favor of outsourcing. He plans on presenting this approach to the Board of Directors as soon as he has made a few more refinements in his presentation.

COO Willy's act of hiring you was, in fact, an act of desperation: the increasing operational dependence on technology services combined with a diminishing IT footprint gravely concerned Mike Willy, and he begged to at least bring in an Information Security expert with the experience necessary to evaluate the current security of GFI's infrastructure and systems. The COO's worst nightmare is a situation where the Confidentiality, Integrity, and Availability of GFI's information systems were compromised – bringing the company to its knees – then having to rely on vendors to pull him out of the mess.

COO Willy has reasons for worrying. GFI has experienced several cyber-attacks from outsiders over the past a few years:

- In 2013, 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 reputation. GFI ended up paying its customers a large sum of settlement for their loss of data confidentiality.
- In 2014, 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. COO Willy isn't sure whether the virus entered GFI's systems through a malicious email, from malware downloaded from the Internet, or via a user's USB flash drive. Regardless of the source of the infection, the company lost $1,700,000 in revenue and intangible customer confidence.

- In a separate incident in 2014, one of the financial consultants left his company laptop unprotected at the airport while travelling and it was stolen. It contained customer financial data and the hard drive was not encrypted. Financial reparations were paid to impacted customers.
- In 2015, a laptop running network sniffer software was found plugged into a network jack under a desk in one of the unoccupied offices.

It is apparent from the number of successful cyber-attacks that GFI is an organization severely lacking in information security maturity. COO Willy has commissioned you to perform a quantitative and qualitative risk assessment of GFI's infrastructure to determine where improvements could be made to reduce the risk of future attacks.

CORPORATE OFFICE NETWORK TOPOLOGY

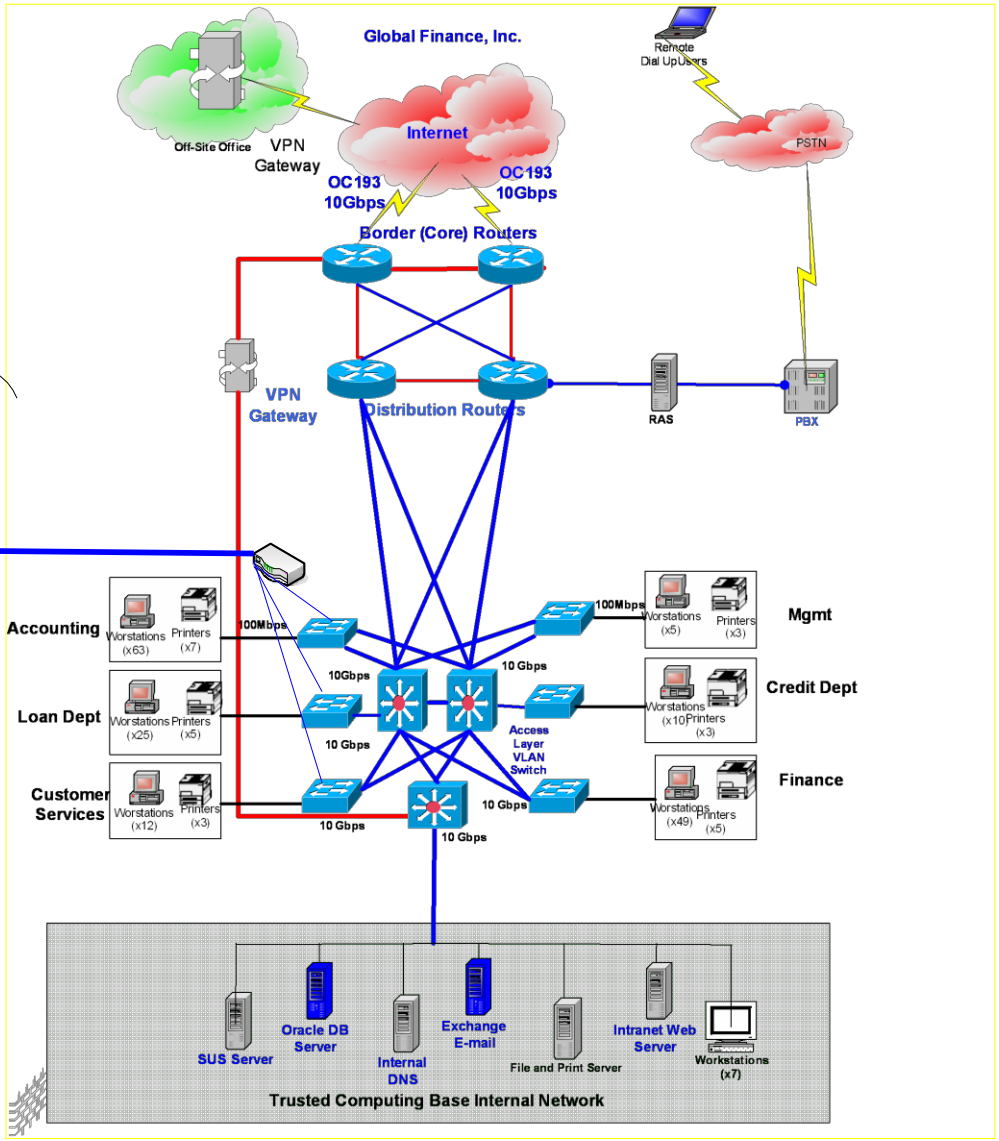
The diagram on the following page displays GFI's Corporate Office Topology.

The GFI network infrastructure consists of a corporate WAN spanning 10 remote facilities that are interconnected to the GFI headquarters' central data processing environment. Data is transmitted from a remote site through a VPN gateway appliance that forms a VPN tunnel with the VPN gateway in headquarters. Through this VPN connection, remote office users access the internal Oracle database to update the customer data tables. Through your inspection of the VPN configuration you discover that the data transaction traversing the remote access connection to the corporate internal databases is not encrypted.

Users are authorized to work from home and both dial-up and VPN remote access are available. Dial-up is provided via Private Branch Exchange (PBX) and a Remote Access Server and VPN remote access is provided via the VPN gateway. Authentication is password-based via MS-CHAP V2. Users are also able to take advantage of GFI's Bring Your Own Device (BYOD) policy and a Wireless antenna allows wireless networking within headquarters. WEP is used to provide wireless security to BYOD users.

The network perimeter between the Internet and GFI's internal network infrastructure is separated by two Border (Core) Routers. These Border Routers then connect to two Distribution Routers and the VPN Gateway. The Distribution Routers connect to a RAS Server, a Wireless Router that provides a bridge between the Wireless Antenna and the internal network, and two Multi-layer switches. The Multilayer switches connect to six (6) Access Layer VLAN switches that segregate the Accounting, Loan Dept, Customer Services, Mgmt, Credit Dept, and Finance VLANs. The Multi-layer switches also connect to a third Multi-layer switch that provides a connection to GFI's servers in the Trusted Computing Base subnet.

The trusted computing based (TCB) internal network is situated in a physically separated subnet. A bulk of the data processing for GFI is handled by an Oracle database on a high end super computer located in the TCB and the TCB also contains an intranet web server used by the internal support team, a Software Update Services (SUS) server used for patch management, an internal DNS server, an e-mail server, and other support personnel workstations. Although each corporate department is segregated physically on a different subnet, they share access to the corporate data in the TCB network.



NOTE: The symbol  represents a multilayer switch

CONSIDERATIONS WHEN CONDUCTING THE RISK ASSESSMENT:

This Risk Assessment and your suggested security improvements are of critical importance. CEO Thompson is set on outsourcing GFI's IT competency and you've been told of a plan from COO Willy to outsource network management and security functions away from your department and over 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 to provide security improvements in certain key areas without a significant increase to the IT budget. It is extremely important that you take into account the value of the assets being protected when selecting security controls to mitigate the risks (i.e. don't spend $1000 to protect an asset worth $500). In addition to what you learned from COO Mike Willy about the previous exploits of GFI's vulnerabilities and what you gathered when reviewing GFI's network infrastructure, the COO has provided some additional information that he wants you to take into account:

1. Ever since an article ran in Fortune about GFI, the 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. Suggestions on improvements to perimeter security and/or methods of identifying the source of intrusions should be presented in your risk assessment.

2. The interrelationship between data and operations concerns COO Mike Willy. Increasingly, some of the ten (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. Suggestions on reducing network latency or increasing application response time and availability should be presented in your risk assessment.

3. Mobility is important for the organization to interact with the customers and other co-workers in near real-time. However, the COO is concerned with mobility security and would like you to research best practices for mobile computing. Security within the BYOD environment should be presented in your risk assessment.

4. Employees enjoy the flexibility of getting access to the corporate network using a WiFi network. However, the COO is concerned over the security ramifications over the wireless network that is widely open to the company and nearby residents. Security within the wireless environment should be presented in your risk assessment.

5. 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 COO is particularly concerned over the cloud computing security in case the customer database is breached.

ASSIGNMENTS

- From the devices and systems identified in the GFI Corporate Network Topology, conduct a thorough asset inventory, assign monetary values to each asset (quantitative), and assign a priority value for each asset (qualitative) that could be used to determine which assets are most critical for restoral in the event of a catastrophic event or attack.
- Evaluate the perimeter security, make a list of access points internal and external (remote), identify vulnerabilities and make suggestions for improvements to perimeter and network security.
- Evaluate the remote access infrastructure, identify vulnerabilities and suggest security improvements to mitigate risks to remote access.
- Address the COO'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.
- Evaluate the authentication protocols and methodologies within the wired, wireless, mobility and remote access environments and suggest improvements to secure authentication for GFI.
- Evaluate the web system protocols and vulnerabilities within the Intranet server and suggest secure protocol improvements to improve security for web authentication.
- Design a cloud computing environment for the company with a secure means of data protection at rest, in motion and in process.
- Assess all known vulnerabilities on each asset in this environment and impacts if compromised.
- Using the asset inventory and the assigned values (monetary and priority) conduct a quantitative and qualitative risk assessment of the GFI network.
- Recommend risk mitigation procedures commensurate with the asset values from your asset inventory. Feel free to redesign the corporate infrastructure and use any combination of technologies to harden the authentication processes and network security measures.
- Provide an Executive Summary.
- You are welcome to make assumptions for any unknown facts as long as you support your assumptions.
- The Title Page, Table of Contents and References page(s) don't count in your 15 page minimum!!!

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 (double-spaced with 12 point font) with APA citations for the resources you used in your research 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. (0)	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. (0)	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. (0)	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. (0)	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. (0)	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. (0)	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)
Evaluate web access protocols and vulnerabilities and Cloud Computing	Did not evaluate web access protocols and vulnerabilities and Cloud Computing (0)	Evaluated web access protocols and vulnerabilities or Cloud Computing. (3)	Evaluated web access protocols and vulnerabilities and Cloud Computing but did not address mission objectives. (6)	Evaluated web access protocols and vulnerabilities and Cloud Computing and addressed mission objectives. (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. (0)	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. (0)	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. (0)	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)