CMIT 425 Advanced Information Systems Security

Risk Assessment Paper

UMUC

Dmitry Landy

March 5, 2020

Risk Assessment Paper

Executive Summary

Global Finance, Inc. (GFI), a financial company, has considered outsourcing as an option to resolve some of the security issues they have encountered. However, this would result in the downsizing of the IT department and result in an increased dependency on third parties or the cloud server providers for security of GFI's system (regarding confidentiality, integrity, and availability). GFI has requested a risk assessment of the GFI corporate network to be conducted what improvements could be made to the GFI corporate network in order to reduce risk of future attacks.

This paper assessed the GFI corporate network in order to determine what issues are present and how to deal with them. The paper is divided into multiple sections that discuss the following:

- Network Perimeter Security
- BYOD Security
- Wireless Security
- VPN Secure Authentication
- Web Security
- Qualitative and Quantitative Assessment
- Risk Mitigation

These sections provide summaries and examples of issues identified or how to identify issues. This paper should not be used as the only source of information to resolve security for the GFI corporate network. This paper should be used as a starting point for securing the network.

Network Perimeter Security

Ensuring the appropriate users have access to a network is absolutely critical. There are many tasks that have to be conducted regarding this, but one is ensuring that the network border is properly prepared. The network border is the outermost layer of the network that is closest to the untrusted or public network. Network perimeter security devices are used in a network to secure that border from outside threats and prevent intrusion or unauthorized access into the private network (Prowse, 2018). There are many security devices that a network can have depending on the security need. This section of the paper will discuss the vulnerabilities associated with the network perimeter and propose possible solutions for improving the network perimeter security.

While analyzing the GFI corporate network, it was found that there was a severe lack of network perimeter devices. Some network perimeter devices that GFI should implement into their network are network and host-based firewall, and network intrusion prevention systems and network intrusion detection systems. Firewalls should be placed right after the border routers to continue where the border routers left off (regarding traffic filtering) (Zelster et al., 2005). Host-based firewalls for servers such as the Oracle database server should definitely be used especially since that was attacked in 2013 and resulted in a significant cost to GFI. Using an IDS or IPS would allow malicious activity to be detected and reported (and stopped if using an IPS). This would provide a significant layer of security. However, these do have monetary costs associated with them and should be considered after conducting a risk assessment of the network. If the cost of implementing the network security device is higher than the benefit, then

it may not be the best idea. However, considering the amount lost due to the Oracle database compromise, that is unlikely.

BYOD Security

The GFI corporate network use of mobile devices within its network provides a mobility advantage which helps in customer and coworker interactions. Additionally, there is a convenience for the employees, reduced hardware costs for GFI, and increased productivity for remote workers (Hoelscher, 2017). However, there are numerous security concerns that are present in a BYOD (bring your own device) environment. This section of the paper will discuss the security concerns with the BYOD environment present in the GFI corporate network.

Since the GFI corporate network uses a BYOD environment, GFI must ensure that it has strong, security-focused policies regarding it. These policies should outline the regulations to be followed, security baseline for the devices prior to connecting to the network, data storage management (personal vs company), device privacy, device update management, device compromise countermeasures, and acceptable use (Veracode, n.d.). Of these areas, device privacy, acceptable use, device compromise countermeasures, and security baseline can present significant security concerns for the network and GFI data (Hoelscher, 2017):

- **Privacy:** There is an inherent privacy concern when using an employee's personal device for company work. Since the device is used within the network, it should be monitored appropriately. The extent of the monitoring should be carefully discussed and decided on by GFI. If the device is not appropriately monitored, it presents a major security risk.

- **Acceptable Use:** Since the device is privately owned by the employees, there needs to be clear distinction as to what it is allowed to be used for and when it is allowed to be used for that. This involves the use of certain apps on the device and how company data (if it's stored on the device) is interacted with (whether by the apps or the user).
- **Device Compromise Countermeasures**: Due to the devices being personally owned by the employees, the devices will have to leave to containment of the GFI office. This mobility makes the devices more prone to being lost. To prepare for this, GFI must ensure that company data stored is appropriately encrypted and that a remote wipe feature is available in case the lost device is not found. Additionally, protocols for reporting the lost or compromised device should be established and the employees should be familiar with it. Depending on the privacy policies regarding BYOD, an app for tracking the devices may be used.
- **Security Baseline:** The security of the device should be treated like any other device on the network (i.e. very seriously). The security of the device will have to be managed by GFI and maintained appropriately. This involves establishing a security baseline for the device before it is allowed on the network. If the device every fails to meet that baseline, an established quarantine procedure should be followed to resolve that issue.

To better maintain BYOD security, CGI must use Mobile Device Management (MDM) software to best manage the devices in a more centralized manner. MDM is software provided by third-party vendors that allows mobile devices to be managed by enforcing password and encryption policies, managing apps, managing inventory of devices, etc. (Rouse & Steele, 2017). This would make device management easier and more secure.

Wireless Security

Wireless access points are a great addition to a network if convenience for connecting to the network is needed or wanted. It allows users to connect to a network without establishing a physical connection using cables. However, a wireless access point does present a variety of security risks that GFI must be aware of since the GFI corporate network includes a wireless router. This section of the paper will discuss the wireless security best practices that GFI should consider to protect their data

When setting up the wireless access point , GFI should ensure that proper authentication methods are in place to keep unauthorized users off of the network. GFI should ensure that WPA2-enterprise, as opposed to WPA2-personal, is being used to authenticate users attempting to gain access (Wilkins, 2011). WPA2-Enterprise uses 802.1X authentication and requires a RADIUS server to authenticate users (SecureW2, n.d.). This is much more secure than WPA or WEP (neither of these should be used). Currently GFI uses WEP for their wireless access point which should be changed to WPA2 immediately. In addition to the authentication, the wireless access point should be ensured to use the appropriate frequency to ensure that range of the AP extends to the appropriate areas. The 5Mhz range is smaller than the 2.4MHz range, which should be considered.

The last consideration is to monitor for any rogue access points and ensure someone does not set one up (Wilkins, 2011). This can cause critical issues for GFI since it has a BYOD policy. If a rogue access point was set up (perhaps to carry out an evil twin attack), company data could be compromised if employees connected to the rogue AP. A rogue AP might accidently be set up

by an employee if they decided to turn on their hotspot. Since the device is likely not appropriately configured to be an access point, an attacker could use it to gather data and/or carry out attacks.

VPN Secure Authentication

Properly establishing rules, regulations, and protocols to ensure appropriate access control for the network is critical (Fahey, R., n.d.). Modern-day attackers have a variety of tools and resources at their disposal to attack a network in an attempt to gain unauthorized access. GFI must be ready to protect their network from those attacks. This does require multiple layers of defense, and ensuring the use of appropriate authentication protocols is one of those layers. This section of the paper will discuss the authentication protocols used in the GFI corporate network and provide suggestions to secure authentication.

The GFI corporate network has various access points that an attacker could exploit for gaining unauthorized access. These access points include remote access points as well. Remote access to a network allows users from remote areas to access the internal network without having to go to the physical network location. This convenience has many security concerns that go with it and can result in significant damage to the network and corporation if they are not addressed properly (University of Nebraska-Lincoln, n.d.).

While analyzing the GFI corporate network, one critical issue present is the lack of encryption found with data transaction traversing the remote access connection to the corporate internal. This issue must be resolved immediately as the information is sensitive and can be seen in plain text by anyone monitoring the network. This is a compromise to data confidentiality and

security. One solution to this is to use IPsec for the VPNs which will ensure that an encrypted tunnel is established and the data transmitted is encrypted as well (Thomas & Elbirt, 2004). IPsec should be used instead of MS-CHAP v2 due to its serious security risks such as vulnerability to dictionary attacks (IVPN, n.d.)

Web Security

An important part of the GIF corporate network is the intranet web server that provides private web services to the network. Since it provides an important functionality, it needs to be properly protected. One of the most important security best practices for any web server is to have a web application firewall (WAF) (Vialle, 2012). This allows traffic to the server to be better filtered to ensure better service and security. Any site that transfers sensitive information must use HTTP with TLS/SSL (HTTPS). This protects the sensitive data by encrypting the transmission. Back-ups of the server should be conducted regularly in case of any issues that result in corrupted data. The server should be updated frequently to minimize vulnerabilities. Lastly, there should be regular antivirus scans being performed on the server to ensure it is safe.

Qualitative and Quantitative Assessment

One of the most important tasks when it comes to managing a network is to assess the network and all that it contains. Global Finance, Inc. (GFI) has a large network spanning 10 remote facilities. Each device in the network plays a specific role and provides a function that varies in levels of importance. Additionally, each device in the network has a monetary value associated with it. These are both factors that have to be considered when properly preparing for a disaster or catastrophe.

This section of the paper will conduct a complete asset inventory of the GFI Corporate network and perform a quantitative and qualitative assessment of that inventory. A quantitative assessment evaluates assets and calculates various values based on the asset in order to determine costs associated with the asset's risks (Gregg, 2005). The resulting values will allow GFI to determine what security measures should or should not be implemented based on the cost. These values can be used by GFI along with the company's budget to determine the most appropriate security solutions surrounding the assets.

A qualitative assessment evaluates assets on their function and purpose, as opposed to their monetary value, in order to rate the importance of the asset (Gregg, 2005). This type of assessment allows GFI to prioritize security measures for assets by evaluating the impact that the asset has on the network and organization. Qualitative assessments do not deal with concrete numbers but in judgment and opinion. This causes this type of assessment to be less exact. However, it is still important to analyze the results of the qualitative assessment to create plans for managing risk.

The following table is an inventory of the GFI Corporate network with the associated monetary value and a priority value. The monetary values describe the cost of the asset while the priority value describes the importance of the device regarding the network. The table will list the items in order of priority (1 being highest, 15 being lowest):

Priority, monetary value, number of assets in network, asset, category

Priority (Qualitative)	**Monetary Value (Quantitative)**	**Asset**	**Number of Assets in the Network**

1	$12,000	Border Routers (e.g. Cisco ASR 9010)	2
2	$1,600	Distribution Router (e.g. Cisco ISR 1921)	2
3	$16,000	Multilayer Switch (e.g. Cisco C9500-16X-A)	3
4	$4,000	Network Switch (e.g. Cisco Catalyst 2960)	6
5	$2/hour	VPN Gateway (e.g. Microsoft Azure)	
6	$400	Wireless Router (e.g. Linksys AC5400)	1
7	$5/user/month	Remote Access Server (RAS)	1
8	$20,000	Oracle Database Server	1
9	$500	Intranet Web Server (e.g. Windows Server 2016 Standard)	1
10	$500	File and Print Server (e.g. Windows Server 2016 Standard)	1
11	$1000/user	Private Branch Exchange (PBX)	1
12	$500 (for hardware)	Internal DNS	1
13	$12/user/month	Exchange Email Server	1
14	$500	SUS Server (e.g. Windows Server 2016 Standard)	1
15	$500	Workstations	174
16	$500	Printers (e.g. Xerox Workcentre 6515)	26

Using the assigned values of the assets, a quantitative and qualitative risk assessment was conducted. Quantitative risk determines values based on the risk, the asset's value, and it's exposure factor. A threat is an event (man-made or natural) that results in a negative impact on

an organization (Gregg, 2005). The following values can be determined based on a threat (Shakeel, n.d.):

- **Exposure Factor (EF):** Percentage of asset lost due to a threat occurring. If the whole asset is completely lost, the EF is 1.0. This number requires some estimation if it is partial.
- **Single Loss Expectancy (SLE):** The the monetary amount lost due to a single occurrence of a threat. This is calculated by EF*asset value
- **Annualized Rate of Occurrence (ARO):** The amount of times the threat will occur throughout the year (12 months). This can be estimated or based on historical data.
- **Annual Loss Expectancy:** The monetary amount lost due to a threat throughout the year. This is determined by SLE * ARO.

The following table is used to show how different threats (1 example per asset) can be assessed to determine a monetary value. The threats and the ARO are based on James Merrit's paper (1999).

Asset	Threat	Asset Value	EF	SLE	ARO	ALE
Border Routers (e.g. Cisco ASR 9010)	Communication Loss	$12,000	.50	$6,000	2	$12,000
Distribution Router (e.g. Cisco ISR 1921)	Power Loss	$1,600	.40	$640	2	$1,280
Multilayer Switch (e.g. Cisco C9500-16X-A)	Earthquake	$16,000	.30	$4,800	.01	$48
Network	Fire to cabling	$4,000	.30	$1,200	.01	$12

Switch (e.g. Cisco Catalyst 2960)						
VPN Gateway (e.g. Microsoft Azure)	Non-disaster downtime	$17,520	.20	$3,504	.06	$210.24
Wireless Router (e.g. Linksys AC5400)	Virus	$400	.1	$40	.68	$27.20
Remote Access Server (RAS)	Accidental Errors	$60/user	.50	$30 /user	.72	$21.60/user
Oracle Database Server	Successful unauthorized system access by outsider	$20,000	1.0	$20,000	.08	$1,600
Intranet Web Server (e.g. Windows Server 2016 Standard)	Non-disaster Downtime	$500	.20	$100	.06	$6
File and Print Server (e.g. Windows Server 2016 Standard)	Power Loss	$500	.20	$100	2	$200
Private Branch Exchange (PBX)	Natural Disaster	$1000/user	.50	$500 /user	.29	$145/user
Internal DNS	Successful Unauthorized System Access by Outsider	$500 (for hardware)	.70	$350	.08	$28
Exchange Email Server	Communication Loss	$144/user	.30	$48/user	2	$96/user
SUS Server	Non-Disaster	$500	.20	$100	.06	$6

(e.g. Windows Server 2016 Standard)	Downtime					
Workstations	Theft	$500	1.0	$500	.24	$120
Printers (e.g. Xerox Workcentre 6515)	Fire	$500	.30	$150	.01	$1.50

A qualitative risk assessment differs from a quantitative risk assessment in that a qualitative assessment determines the likelihood of a threat to an asset and the impact it would have (Gregg, 2005). This is done by taking the identified threats and classifying the impact and probability in appropriate ways, perhaps by low, medium, and high (which is what is used in this assessment). This type of assessment is useful for dealing with things that can't have an exact dollar amount (such as loss of trust). This will allow GFI to determine how threats can impact the organization as a whole or perhaps the network instead of the individual asset.

The following table evaluate a single threat for an asset and determines its probability of occuring and the impact it would have on the organization and network:

Asset	Threat	Probability	Impact
Border Routers (e.g. Cisco ASR 9010)	Communication Loss	High	Med
Distribution Router (e.g. Cisco ISR 1921)	Power Loss	High	Med
Multilayer Switch (e.g. Cisco C9500-16X-A)	Earthquake	Low	Low
Network Switch (e.g.	Fire to cabling	Low	Low

Cisco Catalyst 2960)			
VPN Gateway (e.g. Microsoft Azure)	Non-disaster downtime	Low	Low
Wireless Router (e.g. Linksys AC5400)	Virus	Med	Low
Remote Access Server (RAS)	Accidental Errors	Med	Med
Oracle Database Server	Successful unauthorized system access by outsider	Low	High
Intranet Web Server (e.g. Windows Server 2016 Standard)	Non-disaster Downtime	Low	Low
File and Print Server (e.g. Windows Server 2016 Standard)	Power Loss	High	Low
Private Branch Exchange (PBX)	Natural Disaster	Med	Med
Internal DNS	Successful Unauthorized System Access by Outsider	Low	High
Exchange Email Server	Communication Loss	High	Low
SUS Server (e.g. Windows Server 2016 Standard)	Non-Disaster Downtime	Low	Low
Workstations	Theft	Med	High
Printers (e.g. Xerox Workcentre 6515)	Fire	Low	Low

The probability and impact of the threat can be used in a matrix to determine the overall risk of that threat (Nizhebetskiy, n.d.):

	Low (Impact)	Med (Impact)	High (Impact)
Low (Probability)			
Med (Probability)			
High (Probability)			

- **Yellow:** Risk is overall low and should be kept in mind, but it is not urgent.
- **Orange:** Risk is overall medium and must be monitored and prepared for. Additional analysis should go into the risk.

  Red: Risk is overall high and must thoroughly prepared for and must be well monitored for.

Risk Mitigation

After a risk assessment (qualitative and/or quantitative) has been conducted and the risks are identified appropriately, the next step is to determine how GFI will respond to the risks. Depending on GFI's budget and their priorities, they can use any or all of the following risk mitigation techniques (Gregg, 2005):

- **Risk Reduction:** Implementing something to reduce the risk. One way to do this is by implementing policies to control how something is done or by using more secure protocols. For example, GFI should use IPsec instead of MS-CHAP v2 in order to increase their security which would reduce the risk of compromise in confidentiality.
- **Risk Transference:** This involves transferring risk to someone else, such as through insurance or using the cloud. This could be done by using a cloud service provider to host some of GFI's services.

- **Risk Acceptance:** Conducting a risk assessment and preparing to deal with the risk outcomes.
- **Risk Rejection:** This is ignoring the risk and choosing to do nothing with it. This involved no risk assessment and is extremely dangerous.

After the risk mitigation technique has been decided on, GFI should know that there is still risk left over. This is known as residual risk and it is something that GFI should still prepare for. GFI should evaluate their network and organization after every major change to the infrastructure and plan accordingly.

References

Fahey, R. (n.d.). CISSP Prep: Understanding Access Control. Retrieved from https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/identity-and-access-management/understanding-access-control/

Gregg, M. (2005). CISSP Security-Management Practices. *CISSP Exam Cram 2*. Retrieved from https://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4

Hoelscher, P. (2017). BYOD Security: What are the Risks and How Can They Be Mitigated? Retrieved from https://www.comparitech.com/blog/information-security/byod-security-risks/

IVPN. (n.d.). Comparison of VPN Protocols. Retrieved from https://www.ivpn.net/pptp-vs-ipsec-ikev2-vs-openvpn-vs-wireguard

Meritt, J. W. (1999). A Method for Quantitative Risk Analysis. Retrieved from https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/p28.pdf

Nizhebetskiy, D. (n.d.). Qualitative Risk Analysis Example: How to Perform Risk Assessment. Retrieved from https://pmbasics101.com/how-to-perform-qualitative-risk-analysis/

Prowse, D. (2018). Network Perimeter Security. *CompTIA Security+ SY0-501 Cert Guide, Academic Edition* (2nd Ed.). Retrieved from https://www.pearsonitcertification.com/articles/article.aspx?p=2861447

Rouse, M., & Steele, C. (2017). Mobile Device Management (MDM). Retrieved from https://searchmobilecomputing.techtarget.com/definition/mobile-device-management

SecureW2. (n.d.). Simplifying WPA2-Enterprise and 802.1X. Retrieved from https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified/

Shakeel, I. (n.d.). Risk Management Concepts and the CISSP (Part 1). Retrieved from https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/cissp-risk-management-concepts/

Thomas, J., & Elbirt, J. A. (2004). How IPsec Works, Why We Need It, and Its Biggest Drawbacks. Retrieved from https://www.csoonline.com/article/2117067/data-protection-ipsec.html

University of Nebraska-Lincoln. (n.d.). Remote Access. Retrieved from https://its.unl.edu/bestpractices/remote-access

Veracode. (n.d.). BYOD Security & Policies. Retrieved from https://www.veracode.com/security/byod-security

Vialle, P. (2012). Security Best Practices to Protect Intranet Servers. Retrieved from https://social.technet.microsoft.com/wiki/contents/articles/12931.security-best-practices-to-protect-intranet-servers.aspx

Wilkins, S. (2011). Wireless Security Considerations: Common Security Threats to Wireless Networks. Retrieved from https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats

Zelser, L. et al. (2005). Perimeter Security Fundamentals. Inside Network perimeter Security (2nd Ed.). Retrieved from https://www.informit.com/articles/article.aspx?p=376256