Risk Management Plan for DHAEI

By: Danielle Daza

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This risk management plan has been developed with the intent to be NIST-compliant. With the NIST Risk Management Framework (RMF) being a US federal government guideline, standard and process for managing risk, it was used as a template for analyzing the risks apparent in DHAEI's current data environment. Within this report are sections dedicated to the first three steps of the NIST RMF - Prepare, Categorize, Select. Under the Prepare step, suggested lines of communications in implementing risk-managing strategies and defined risk management roles for accountability have been prepared. This will allow for clear communications across the most relevant departments about the general security posture and how as a company the risks are being addressed and how. Under the Categorize step, a thorough quantitative risk assessment of the most at-risk assets has been compiled as well as a summary table for who would be the risk owners of the risks that have been discussed. The risks in question mainly relate to the remote and on-site network infrastructures and methods in which critical data is stored and protected. After a comprehensive review of the risks of most consequence and a clear understanding of the individuals that would be best suited to address those risks, an accurate selection of controls for the risks can begin to be implemented. As such, the best-suited controls for the risks addressed in this report have been recommended and explored in detail under the Select step. Both general controls and risk-specific controls have been provided to more holistically approach the risks.

OBJECTIVES

PURPOSE

In order to best cover all bases when developing this Risk Management Plan, the NIST Risk Management Framework (RMF) has been used as a guide in understanding how to best proceed with the planned changes while being aware of the realistic risks that need prioritized attention.

A summary of the NIST RMF has been provided below for reference:

Stage	Description	Expected Outcomes
Prepare	Essential activities to prepare the organization to manage security and privacy risks (NIST Risk Management Framework RMF, 2024)	1. Identify key risk management roles 2. Organizational risk management strategy developed and fully adopted within the company a. Risk and security employee training 3. Organization-wide strategy for continuous monitoring
Categorize	Categorize the system and information processed, stored, and transmitted based on an impact analysis (NIST Risk Management Framework RMF, 2024)	4. Security categorization of system and information assets 5. Categorization decisions reviewed and approved by authorized individuals within the company
Select	Select the set of NIST SP 800-53 controls to protect the system based on risk assessments (NIST Risk Management Framework RMF, 2024)	6. Control baselines tailored to company needs 7. Controls allocated to specific system components 8. Continuous monitoring strategy established system-level
Implement	Implement the controls and document how controls are deployed (NIST Risk Management Framework RMF, 2024)	9. Implement approved controls specified in security and privacy plans a. E.g. establish identity and access management (IAM) controls to easily identify who has access to data, systems, and networks. 10. Implemented controls' performance is reviewed
Assess	Assess to determine if the controls are in place, operating as intended, and producing the desired results (NIST Risk Management Framework RMF, 2024)	11. Establish an assessor or assessment team to ensure the efficiency of the security implementations 12. Assessment plans development, reviewed, approved 13. Appropriate remediation actions to address faults in controls are taken

		14. Continual updates to security and privacy plans are made to reflect implementation changes in the assessment stage 15. Plans of actions and milestone goals are developed as the company ambitions and systems evolve
Authorize	Senior official makes a risk-based decision to authorize the system (to operate) (NIST Risk Management Framework RMF, 2024)	16. Provide accountability by requiring a senior official to determine if security and privacy plans are acceptable 17. Risk determination rendered and risk responses provided 18. Authorization of system or common controls are approved or denied and revised
Monitor	Continuously monitor control implementation and risks to the system (NIST Risk Management Framework RMF, 2024)	19. System operations monitored in accordance with continuous monitoring strategy 20. Using the continuous monitoring strategy as a guide, conduct ongoing assessments of control effectiveness 21. Output of continuous monitoring activities routinely analyzed and responded to

This report aims to cover the bases of the first three steps of the NIST RMF – Prepare, Categorize, and Select. After reviewing this report and further discussion on how to best proceed given the provided information, plans towards the next stages of this framework may begin.

SCOPE

The scope of this Risk Management Plan has been made with the information given about the current state of the company's technological standing and history as well as its plans for expansion. Apparent in this report is an emphasis on the planned changes in regards to the technical, security and user requirements outlined.

If there is an oversight in regards to the scope that this report has examined or any specific information that is needed to be considered that is not observed to have been within this report, it is recommended that it be discussed in a timely manner and the controls selected be adjusted accordingly.

PREPARE

This section will establish a recommendation of groundwork to set in terms of lines of communication relating to information security and the risks associated with its assets.

COMMUNICATION LINES

Below is a table summarizing the individuals recommended to keep generally aware of the risks addressed and the controls recommended to implement.

Name	Title	Rationale
Alan Hake	Founder, CEO	So as to be aware of the risks observed in his company and have final say on the plans for mitigating the risks addressed.
Richard Xavier	COO	As the COO's main task being making operational decisions that align with the company's strategy and goals, they should have an awareness of the company's risks and threats in all relevant aspects of the company – including information security – in order to best ensure the success of a business' long-term ambitions through contingency plans and overseeing the implementations of necessary controls.
Rachel Xieng	CFO	As the risks of the company may also relate to data integrity, it would also be of interest of the CFO to at least be basically aware of the specific risks present in the current network and of what the controls suggested would mitigate such risks.
Cecilia Thompson	Mgr. Networking	This position would need to be kept aware of risk related discussions in order to best manage the team under her supervision that would be directly involved in implementing the necessary security controls necessary.

Below is a table summarizing the individuals recommended to be directly be involved in the processing of the selecting controls and monitoring the controls' performance.

Name	Title	Rationale
Amanda Wilson	CIO	As the CIO is responsible for overseeing the information technology department's resources and staff, being aware of the risks present, especially the risks in the IT department, would be essential in her duties in developing and implementing the organization's entire IT strategy (WoollacottEmma, 2024). Of all the senior executives, the CIO

		would be expected to be most involved and kept most up-to-date, if not at least overseeing the progress of the controls being selected and implemented.
Paul Alexander	CISO	Directly under the CIO, the expectations of a CISO is to continuously develop, implement, and enforce security policies to protect the company's critical data. As such, it is natural for this position to be the most involved in the oversight of implementing the necessary controls regarding the risks to be outlined in this report.
Harold Fry	Security Technician	As this position is currently the only position under the CISO, it is imperative that this position be well-aware of the risks present in the company as well as understand the implications of such risks in the scope of the entire company. In order to best select ad implement the necessary controls, the Security Technician needs to be well-informed of the company's current technological environment and the implications of the plans that have been established.
Scotty Doohan	Mgr. Applications	This position would need to be involved in managing application-level security optimization and access control for the company's risks. Though his team would be more directly involved, this position would play an important role in ensuring that control requirements are being met.
William Freund	Mgr. Systems	This position would oversee several positions that would need to be, in some capacity, involved in the implementation of controls that would address the current risks evident in the system infrastructure. As such, would most likely be more directly involved in the process than other department managers.
Vincent DiSalvo	Network Architect	With the planned changes being heavily reliant on the success of meeting specified technical requirements, the process of doing so and ensuring the security of the information remains intact calls for the attention of a network architect to best design the data communication networks needed to align with the business needs as well as mitigating as much risk in the process.

KEY RISK MANAGEMENT ROLES

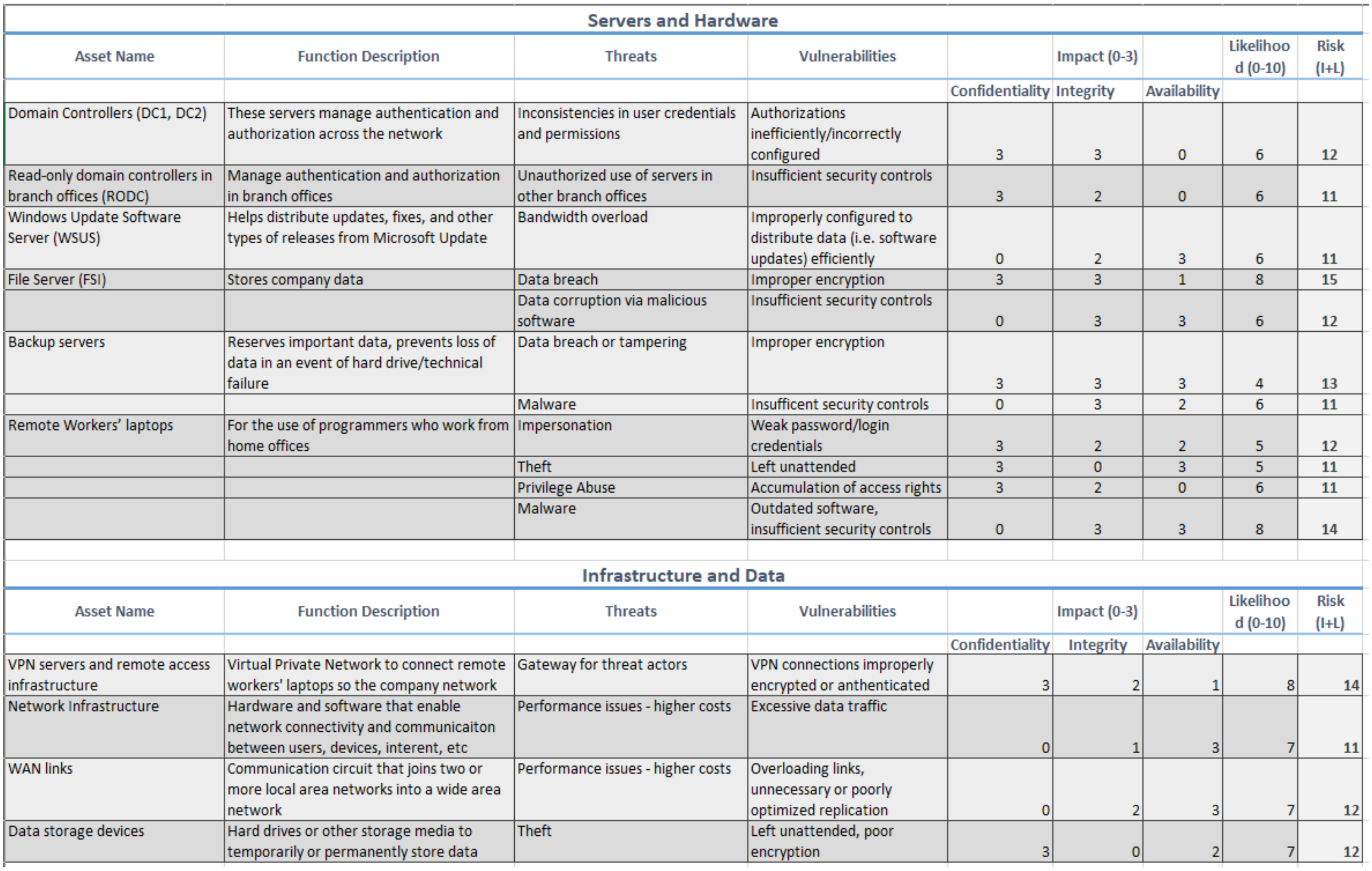
As the previous section summarized the recommended lines of communication in the process of implementing this Risk Management Plan, below will outline the key risk management roles based on the rationale explained in the previous section.

Name	Title	Capacity of Responsibility

Amanda Wilson	CIO	Ultimate decision-making and guidance in determining appropriate controls (NIST RMF Roles and Responsibilities Crosswalk, 20204).
Paul Alexander	CISO	Overall management and implementation of necessary controls (NIST RMF Roles and Responsibilities Crosswalk, 20204).
Harold Fry	Security Technician	Direct implementation, assessment and monitoring of controls as well as provide additional recommendations based on his observations. Whenever there is another security technician to fill the vacant position, this would be a shared responsibility between the two (NIST RMF Roles and Responsibilities Crosswalk, 20204).

CATEGORIZE

This section will delve into the Categorize step in the outlined NIST Risk Management Framework. This includes conducting a risk assessment on the most valuable assets of the organization, and narrowing down the main areas of concern to address first while determining which risks are not of highest priority.



Servers and Hardware

Asset Name	Function Description	Threats	Vulnerabilities		Impact (0-3)		Likelihood (0-10)	Risk (I+L)
				Confidentiality	Integrity	Availability		
Domain Controllers (DC1, DC2)	These servers manage authentication and authorization across the network	Inconsistencies in user credentials and permissions	Authorizations inefficiently/incorrectly configured	3	3	0	6	12
Read-only domain controllers in branch offices (RODC)	Manage authentication and authorization in branch offices	Unauthorized use of servers in other branch offices	Insufficient security controls	3	2	0	6	11
Windows Update Software Server (WSUS)	Helps distribute updates, fixes, and other types of releases from Microsoft Update	Bandwidth overload	Improperly configured to distribute data (i.e. software updates) efficiently	0	2	3	6	11
File Server (FSI)	Stores company data	Data breach	Improper encryption	3	3	1	8	15
		Data corruption via malicious software	Insufficient security controls	0	3	3	6	12
Backup servers	Reserves important data, prevents loss of data in an event of hard drive/technical failure	Data breach or tampering	Improper encryption	3	3	3	4	13
		Malware	Insufficent security controls	0	3	2	6	11
Remote Workers' laptops	For the use of programmers who work from home offices	Impersonation	Weak password/login credentials	3	2	2	5	12
		Theft	Left unattended	3	0	3	5	11
		Privilege Abuse	Accumulation of access rights	3	2	0	6	11
		Malware	Outdated software, insufficient security controls	0	3	3	8	14

Infrastructure and Data

Asset Name	Function Description	Threats	Vulnerabilities		Impact (0-3)		Likelihood (0-10)	Risk (I+L)
				Confidentiality	Integrity	Availability		
VPN servers and remote access infrastructure	Virtual Private Network to connect remote workers' laptops so the company network	Gateway for threat actors	VPN connections improperly encrypted or anthenticated	3	2	1	8	14
Network Infrastructure	Hardware and software that enable network connectivity and communicaiton between users, devices, interent, etc	Performance issues - higher costs	Excessive data traffic	0	1	3	7	11
WAN links	Communication circuit that joins two or more local area networks into a wide area network	Performance issues - higher costs	Overloading links, unnecessary or poorly optimized replication	0	2	3	7	12
Data storage devices	Hard drives or other storage media to temporarily or permanently store data	Theft	Left unattended, poor encryption	3	0	2	7	12

The analysis of the company's main assets of major consequence have been summarized in the tables in the following section. This includes an assessment of the threats and relevant vulnerabilities involved with each asset as well as a numerical value placed on the potential impact and likelihoods of those threats occurring which result in a numerical value in evaluating the priority of those risks.

As the risks assessed are the main assets of major consequence, the risk observable is quite high with few threats being completely "ignorable". However, for the sake of approaching these risks in a holistic way, the risks have been encapsulated into four main risks of concern. The four risks have been summarized below along with the specific assets the risks include.

Risk	Relevant Assets	Description
Unauthorized Access to Systems and Data	- Remote workers' laptops - Branch office servers - VPN servers and network infrastructure	Remote workers and branch office technicians may gain unauthorized access to critical systems or data if access controls are not properly enforced.
Data Breaches and Theft from Servers	- File servers - Data storage devices - Backup servers/systems	Sensitive data stored on file and backup servers could be exposed if servers are compromised or corrupted.
Inefficient Use of Bandwidth and VPN Overload – Performance Issues	- Network infrastructure - VPC servers and remote access infrastructure - File servers and WSUS server (update distribution)	Excessive VPN usage and large data transfers could overload the company's network, especially current remote worker connections and the new branch office setups.
Active Directory Replication Issues – Data Consistency and WAN Bandwidth	- Active directory servers, domain controllers (DC1, DC2, branch office RODCs) - WAN links - Network infrastructure	The new branch office setup, including RODCs, could lead to inefficient Active Directory replication across WAN links, impacting data consistency and network performance.

RISK OWNERS

Risk	Primary Risk Owner	Rationale	Additional contributors
Unauthorized Access to Systems and Data	CISO and CIO in some capacity	Ultimately responsible for information security across organization. However, CIO would also play a role in decisions regarding network and system architecture (NIST RMF Roles and Responsibilities Crosswalk, 20204).	- IT support technicians – configurations and maintenance of remote access systems. - Network architect and team – securing and optimizing VPNs, firewalls, network monitoring tools.
Data Breaches and Theft from Servers	CISO	Oversees all aspects of information security and is responsible for establishing controls such as encryption and backup strategies for the file servers (NIST RMF Roles and Responsibilities Crosswalk, 20204).	- System administrator – directly responsible for implementing technical solutions that would best suit company needs. - Security technician(s) – responsible for monitoring the security of the servers and ensuring patches are applied regularly.
Inefficient Use of Bandwidth and VPN Overload –	Network Administrator and CIO in some capacity	The issue lies with company network performance, including VPN, WAN, and internal network optimizations. Again, the CIO should oversee	- Network architect and team – ensuring the infrastructure is optimized (WAN, VPN load balancing).

Performance Issues		the performance goals (NIST RMF Roles and Responsibilities Crosswalk, 20204).	- IT support technicians – monitoring VPN usage and apply best changes for managing performance. - CISO – work in collaboration with the network team to ensure security controls do not impede network performance.
Active Directory Replication Issues – Data Consistency and WAN Bandwidth	Network Administrator	Work to optimize WAN bandwidth and ensure efficient replication (NIST RMF Roles and Responsibilities Crosswalk, 20204).	- CISO – ensure that security policies are maintained during the replication process. - IT technicians at branch offices – work in collaboration with network team to ensure the RODCs in the branch offices are correctly configured and replicating efficiently with minimal bandwidth usage.

RISK ACCEPTANCE CRITERIA

Evident from the table above, there certain threats that are not addressed as substantial risks in the following sections. This is due to the current threat landscape in that there is a generally higher likelihood of compromise of information systems and networks through, for example, malware rather than physical theft (Cybersecurity Risks, 2023). Though the consequences of certain threats are substantial, if the likelihood is relatively low (i.e. 5 or below), it is an acceptable risk in comparison to the other apparent risks present within the company's infrastructure.

SELECT (RISK TREATMENT)

GENERAL CONTROLS TO CONSIDER

The following controls have been provided in order of priority to address the current state of the security posture of DHAEI. These controls would also have an effect in addressing the specifically discussed risks.

1. CA-7: Continuous Monitoring
    - Develop a system-level continuous monitoring strategy to detect any unusual activities to ensure timely responses to potential threats (Ross, 2020, p.90-91)
2. AC-6: Least Privilege
    - Employ the principle of least privilege, granting users, technicians, and administrators the minimum level of access required to perform their tasks (Ross, 2020, p.36-37)
3. IR-4: Incident Handling
    - Establish and maintain an incident response plan to respond to security incidents quickly and effectively, minimizing downtime and potential damage (Ross, 2020, p. 152)
    - Coordinate incident handling activities with contingency planning activities (Ross, 2020, p. 152)
4. SI-4: System Monitoring
    - Continuously monitoring the system's health and performance to detect any issues in real time such as hardware failures, unauthorized access, or performance bottlenecks (Ross, 2020, p.336-337)

UNAUTHORIZED ACCESS TO SYSTEMS AND DATA

The following controls have been provided to address the specific risk of unauthorized access of systems and data.

1. AC-2: Account Management
    - Define and document the types of accounts allowed and specifically prohibited for use within the system (Ross, 2020, p.19)

- Specify authorized users of the system, role and group membership and access authorizations for each account to ensure technicians and remote users have only the necessary access to perform their tasks (least privilege principle)

2. AC-17: Remote Access
   - Establish and document usage restrictions, connection and configuration connection requirements, and implementation guidance for each type of remote access allowed (Ross, 2020, p. 48)
   - Ensure that remote access is secure and strictly managed
   - Enforcing encrypted VPN connections and multi-factor authentication (MFA) for all remote workers
3. AC-19: Access Control for Mobile Devices
   - Establish configuration and connection requirements and implementation guidance for organization-controlled mobile devices
   - Apply mobile device management (MDM) solutions and ensure endpoint protection, including encryption and strong authentication for the company-issued laptops (Ross, 2020, p. 51-52)
4. IA-2: Identification and Authentication
   - Uniquely identify organizational users and associate that unique identification with processes acting on behalf of those users such as MFA to ensure credentials are not easily compromised (Ross, 2020, p. 132)

DATA BREACHES AND THEFT FROM SERVERS

The following controls have been provided to address the specific risk of data breaches and theft from servers.

1. CP-9: Information System Backup

- Conduct regular backups of critical data in an encrypted format, either on or off-site to mitigate data loss in the case of a hardware failure or compromise (Ross, 2020, p. 125-126)

2. CP-10: System Recovery and Reconstitution
   - Develop and test disaster recovery plans to ensure that critical data can be quickly restored after an incident (Ross, 2020, p. 128)
3. SC-28: Protection of Information at Rest
   - Ensure that the data on servers is encrypted to protect sensitive data in case of compromise (Ross, 2020, p. 316-317)

INEFFICIENT USE OF BANDWIDTH AND VPN OVERLOAD – PERFORMANCE ISSUES

The following controls have been provided to address the specific risk of inefficient use of bandwidth and VPN overload.

1. SC-5: Denial of Service Protection
   - Implement DoS protection mechanisms to ensure network resources are not overwhelmed by excessive traffic (Ross, 2020, p. 296)
2. SC-7: Boundary Protection
   - Monitor and control communications at the external managed interfaces to the system and at key internally-managed interfaces within the system (Ross, 2020, p. 297-298)
   - Utilizing firewalls, intrusion prevention systems (IPS) and traffic filtering to prioritize critical traffic and reduce network congestion
3. SC-12: Cryptographic Key Establishment and Management
   - Establish and manage cryptographic keys in order to secure VPN traffic with encryption to prevent overloading the bandwidth which may be caused by

unauthorized data interceptions or man-in-the-middle attacks (Ross, 2020, p. 307-308)

ACTIVE DIRECTORY REPLICATION ISSUES

The following controls have been provided to address the specific risk of active directory replication issues

1. IA-2: Identification and Authentication
   - As explained in an earlier section, this control could also be used in ensuring strong authentication methods for any replication activities and ensuring that the RODCs only store necessary information without compromising security (Ross, 2020, p. 132)
2. IA-5: Authenticator Management
   - Securely manage system authenticators by (Ross, 2020, p. 138-139)
     i. Verifying the identity of the individual, group, role, service, or device receiving the authenticator
     ii. Establishing and implementing administrative procedures for initial authenticator distribution for lost or compromised authenticators
   - Protect credentials use in replication processes by ensuring they are not stored on RODCs or outside company-controlled systems
3. CP-10: System Recovery and Reconstitution (Ross, 2020, p. 128)
   - Provide for the recovery and reconstitution of the system to a known state within the organization
   - Ensure Active Directory replication is optimized by scheduling it during off-peak hours to ensure that there is a minimal impact on the WAN bandwidth
4. SC-7: Boundary Protection (Ross, 2020, p.297-298)

- As explained in an earlier section, this control could be implemented in applying the necessary policies to prioritize essential traffic such as Active Directory replication, ensuring minimal impact on the network

REFERENCES

Cybersecurity Risks. (2023, November 3). Retrieved from NIST: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/cybersecurity-risks

NIST Risk Management Framework RMF. (2024, September 24). Retrieved from National Vulnerabilities Database: https://csrc.nist.gov/projects/risk-management/about-rmf

NIST RMF Roles and Responsibilities Crosswalk. (20204, September). Retrieved from NIST Information Technology Laboratory: https://csrc.nist.gov/csrc/media/Projects/risk-management/documents/Additional%20Resources/NIST%20RMF%20Roles%20and%20Responsibilities%20Crosswalk.pdf

Planning Domain Controller Placement. (2024, November 11). Retrieved from Microsoft: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/planning-domain-controller-placement

Ross, W. L. (2020). Security and Privacy Controls for Information Systems and Organizations. *NIST Special Publication 800-53 Revision 5*, 19, 36-37, 48, 50-51, 90-91, 125-126, , 15128, 132, 138-139, 152, 296, 297-298, 307-308, 316-317, 336-337.

Woollacott, E. (2024, March 19). *What Is A Chief Information Officer? CIO Role Explained*. Retrieved from Forbes: https://www.forbes.com/sites/emmawoollacott/article/chief-information-officer-cio/