Security Overview: Phishing, Social Engineering, Authentication with —-------

Joshua J. Simpson

Western Governors University

Summary

---------- is a growing digital marketing and consulting business. As the company has expanded, it has faced an increasing number of attempts to exfiltrate data and infiltrate its internal systems. In the early years, ---------- experienced 2 or 3 compromise attempts annually, ranging from social engineering to network infiltration. However, with the company's growth, these attempts have surged by 532%. Of this increase, 36.2% of the attempts have impacted ----------, harming both its reputation and its customers.

Conducting a comprehensive analysis of ----------'s systems and implementing controls and safeguards highlights the importance of proper security implementation. Through collaboration, the implementation of these "deliverables" provided an in-depth understanding of how to enhance the organization’s security posture.

---------- will face significant challenges that necessitate the implementation of robust security measures. As an online agency dealing with sensitive information, including proprietary business data and credit card details, ensuring data protection will be paramount. Over the next three years, ---------- is expected to experience 200% growth, expanding its team and diversifying its consulting and training services.

Without comprehensive security controls, ---------- will likely face weekly security breaches, leading to frequent data exfiltration and unauthorized data alterations. These breaches will damage the company's reputation and incur financial penalties, highlighting the urgent need for a more secure and resilient infrastructure.

The necessity for implementing a comprehensive Security Awareness Training and Education (SATE) program will be driven by the low initial awareness of cybersecurity threats among employees, currently at only 45%. Enhancing this awareness to 90% will be crucial for building a security culture within the organization.

Deploying Zscaler and Barracuda Sentinel will also be critical. Prior to these implementations, ---------- will experience frequent malware incidents and phishing attempts, compromising the integrity of its network and email communications. Implementing Zscaler's cloud-based security solutions will reduce malware incidents by 86%, while Barracuda Sentinel’s advanced email security features will decrease phishing attempts by 75%.

Ultimately, ----------’s overall security maturity is currently assessed at a mere 30%. To protect their expanding business and maintain the trust of their clients, it will be imperative to increase this security level. The comprehensive measures to be taken,

including advanced security solutions and targeted employee training, will elevate ----------'s security level to an impressive 98%. This transformation will underscore the vital need for strategic security planning and implementation in mitigating risks and safeguarding organizational assets.

Review of work orders

Work order #1

This study aims to determine the effectiveness of Multi-factor Authentication (MFA) in deterring cyber crimes. Microsoft's study was titled "How Effective is Multi-factor Authentication at Deterring Cyberattacks?" to underscore the significance of MFA in daily operations. It compares the security of accounts with and without MFA, demonstrating that accounts with MFA exhibit outstanding protection, reducing the risk of compromise by 96.22%.

Implementing various identification methods for personnel, such as combining a keycard (Something the user has) with a password (Something the user knows), significantly hinders attackers from gaining access to both credentials. This approach strengthens security parameters, creating a more secure barrier against unauthorized entry. Therefore, MFA plays a crucial role in all organizations, acting as a fail-safe

mechanism. Even if a password is stolen, it is only one piece of the authentication process, preventing malicious individuals from accessing the network.

There are numerous MFA software options available. For ----------, we will implement "Microsoft Entra Multi-factor Authentication." This software employs three forms of authentication, ensuring a secure access policy. Additionally, Microsoft provides robust support for this software, aligning with ---------- requirements for ease of use.

Work order #2

This work order focuses on integrating anti-phishing software into the ---------- network. A study by Emily Jones titled "Anti-Phishing Software: Does It Protect Companies?" highlights the critical importance of such measures. Phishing has existed since the mid-1990s, has evolved in complexity, and now infiltrates various aspects of our lives. It is essential to protect organizations from these diverse threats by implementing robust anti-phishing software.

A study includes an anonymous quote stating, "Phishing emails have quickly become the most common delivery method for ransomware, which can wreak havoc on any size business. So, any prevention against phishing can also protect your business

from serious cyber issues." This emphasizes the critical need for robust anti-phishing measures.

One of the recent most notorious phishing attacks targeted Colonial Pipeline in 2021. The attackers extorted $4.4 million by locking Colonial Pipeline out of their systems. Although this ransom might seem relatively small, the broader impact was devastating. The entire operation was shut down, halting revenue generation and resulting in total losses estimated at around USD 3.7 billion.

This incident underscores the importance of protecting business email systems from malicious actors. Organizations can safeguard themselves against significant financial and operational disruptions by preventing phishing attacks by 75%.

---------- will be implementing Barracuda Sentinel**.** Barracuda Sentinel is an anti-phishing software that works with Office 365. It uses AI to sort through risky emails. It uses a massive database to compare emails and ensures that most bad emails do not even reach the inbox.

Work order #3

This work order is dedicated to establishing a zero-trust network architecture. The concept of zero trust is comprehensively discussed in a blog by CYBERARK titled "What Is Zero Trust and Why Is it So Important?" Zero trust is a strategic cybersecurity model designed to secure modern digital business environments by permitting only authorized processes and individuals to access the network. This approach significantly enhances the network's defense-in-depth strategy, resulting in a more robust and resilient security posture.

Zero trust is a multifaceted concept crucial for fortifying organizational defenses against evolving threats. While it enhances security significantly, it also introduces challenges by potentially limiting accessibility and agility in responding to operational needs. The principles outlined in a recent blog post underscore vital components essential to any robust zero-trust system.

Firstly, "Strong, adaptive authentication," akin to Multi-factor Authentication (MFA) discussed earlier (see pg. 4), forms the foundational pillar of verifying user identities securely. Secondly, "Continuous approval and authorization" mandates periodic revalidation of user permissions to ensure that only authorized individuals retain access

privileges. The third principle, "Secure, least privilege access," restricts user visibility to only the necessary information pertinent to their roles, bolstering data protection.

Moreover, "Continuously monitor and attest" involves ongoing scrutiny for anomalies, preemptively thwarting potential threats before they escalate. Lastly, "Credential and authentication protection" focuses on safeguarding endpoint integrity and thwarting attempts to exploit sensitive data. This comprehensive approach illustrates how zero trust enables a defense-in-depth strategy, augmenting overall organizational security.

Delving deeper into these principles reveals that zero trust reinforces cybersecurity resilience and promotes a proactive stance against emerging threats. By embracing these principles, organizations can cultivate a robust security posture that adapts and evolves with the dynamic threat landscape, safeguarding critical assets and maintaining operational continuity effectively and increasing 86%.

For —--------, we plan to implement Zscaler. Zscaler provides zero trust and better overall security using internal and external resources.

Work order #4

This work order focuses on training personnel and implementing programs to enhance their ability to identify and avoid abnormalities, particularly suspicious links or emails. Security Awareness Training and Education (SATE) programs equip employees with the knowledge to make informed decisions regarding cybersecurity best practices. The referenced study by MARINER, titled "Security Awareness Training: What It Is and Why You Need It," underscores the importance of educating personnel about security threats. Human error remains the primary cause of cyber incidents worldwide, whether due to clicking on malicious links or neglecting timely software updates. Effective SATE Training addresses these challenges by imparting essential knowledge and skills to mitigate risks.

Investing in people is not just a commitment but a strategic imperative, particularly when safeguarding an organization's integrity and resilience. ---------- has embraced this ethos wholeheartedly, understanding that the competence and awareness of its workforce are pivotal in ensuring operational security. This realization has been underscored by recent insights, such as the revelation in a prominent blog post that over 90% of security breaches result from human errors. Armed with this awareness, ---------- is actively pursuing measures to mitigate such risks by addressing potential gaps in knowledge and awareness among its staff, protecting from human error 96%.

Central to ----------'s strategy is a proactive approach to training and development. By investing in comprehensive programs that equip employees with the latest security protocols and foster a culture of accountability and vigilance, the company aims to fortify its defenses against cyber threats. These initiatives are not merely reactionary but forward-thinking, striving to instill a deep-rooted understanding of cybersecurity best practices throughout the organization. Through continuous education and reinforcement, ---------- seeks to empower its workforce to identify and mitigate risks proactively, thereby enhancing organizational resilience and safeguarding its reputation in an increasingly digital landscape.

Change to Project Environment

Original environments

The current project environment at ---------- encompasses several components that can be distributed across multiple management and IT groups.

- Administrative Controls
- Policy and Procedures
- Technical Controls
- IT Infrastructures

---------- has encountered numerous challenges stemming from a need for robust security controls and comprehensive policies. This deficiency has led to significant issues, including frequent data exfiltration incidents and unauthorized data alterations. The absence of adequate security measures and insufficient employee training has resulted in a recurring pattern of security breaches every week. These incidents not only damage the company's reputation but also lead to substantial financial penalties.

A recent example highlights the severity of these issues: last month, an employee was deceived by a phishing email that directed him to a counterfeit login page. The email, masquerading as an urgent communication about "critical updates," prompted the employee to enter his credentials, which were subsequently stolen. The attackers used these credentials to alter sensitive data within the company's database, demonstrating the urgent need for improved security protocols and employee training.

To address these challenges, it is imperative for ---------- to conduct a thorough review and overhaul of its current security controls and training programs. Implementing more robust security measures and comprehensive training will protect the company's sensitive data and safeguard its reputation and financial stability.

---------- operates with a diverse IT infrastructure, including multiple servers hosting production environments, databases, and public cloud infrastructures. The company employs a multitiered network architecture to support office-based and remote work environments. Remote employees' devices are fully encrypted and connected to the ---------- network via a Virtual Private Network (VPN), granting them secure access to internal servers. In-office employees use cabled connections for enhanced security, and their workstations are fully encrypted to protect against unauthorized access.

---------- employs Single Sign-On (SSO) technology to manage access control effectively. This ensures that only employees with the correct credentials can access the internal network and associated servers. Additionally, endpoint protection software is installed on all workstations to monitor for and block viruses and malware, providing an additional layer of security.

The company's network infrastructure is meticulously segmented to ensure security and operational efficiency. Visitors and customers are granted access to an external-facing network, while contractors are restricted to the extranet. All wired connections within the office are part of a secure intranet, ensuring that sensitive information is accessible only to those with a legitimate need to know. ---------- also

employs MAC address whitelisting to prevent unauthorized devices from joining the network, further enhancing security.

To bolster network security, ---------- utilizes an Intrusion Prevention System (IPS) that monitors network traffic for suspicious activity. This system, combined with a layer 4 firewall, oversees the transport of data packets across the network, ensuring that only legitimate traffic is allowed. These measures help to protect the company's network from external threats and unauthorized access.

In addition to digital security measures, ---------- has implemented stringent physical security protocols. Bollards are installed at the front and rear entrances to prevent unauthorized vehicle access. Spot.AI cameras are strategically placed to monitor workplace activity and secure areas, providing real-time surveillance and recording capabilities. The company's entry system includes dual doors requiring key card access, creating an authorized entrance, and a mantrap that prevents unauthorized access. Sensitive areas within the office, such as server rooms and corporate offices, are secured with additional key card access controls, ensuring that only authorized personnel can enter.

By addressing these security weaknesses and implementing comprehensive security controls and training programs, ---------- aims to create a more secure and resilient environment. This proactive approach will protect the company's valuable data, maintain its reputation, and ensure the safety and trust of its customers in an increasingly complex threat landscape.

Expected environment Post-project implementation

Implementation and Impact: By adopting MFA, ---------- has significantly bolstered its security posture. The company has implemented Microsoft Entra Multi-factor Authentication, which uses three forms of authentication to ensure secure access. This solution meets the company's requirements for ease of use and integrates seamlessly with their existing infrastructure.

MFA combines multiple identification methods, such as a keycard (Something the user has) and a password (Something the user knows), creating a robust barrier against unauthorized access. This layered approach ensures that even if a password is stolen, it alone is insufficient for network entry. As a result, ---------- has seen a substantial decrease in unauthorized access attempts, leading to improved security and reduced risk of data breaches by 92.3%.

Implementation and Impact: ---------- has integrated Barracuda Sentinel, an advanced anti-phishing software that works seamlessly with Office 365. Barracuda Sentinel uses

artificial intelligence to analyze and filter out risky emails, preventing them from reaching employees' inboxes. This proactive approach significantly reduces the likelihood of phishing attacks, thereby protecting the company from potential financial and operational disruptions.

By implementing Barracuda Sentinel, ---------- has created a more secure email environment. The software's ability to identify and block malicious emails before they reach employees has drastically reduced the number of phishing incidents. Consequently, the company has experienced fewer security breaches, enhanced operational stability, and greater employee confidence in the security of their communications by 75%.

Implementation and Impact: ---------- has adopted Zscaler to implement a Zero Trust architecture. Zscaler's platform ensures that only authorized processes and individuals can access the network, enhancing overall security. The key principles of Zero Trust—robust and adaptive authentication, continuous approval and authorization, least privilege access, continuous monitoring, and credential protection—are all integral to this implementation.

The adoption of Zero Trust has transformed ----------'s security landscape. The company has created a dynamic and secure environment by restricting access to only

what is necessary and continuously monitoring for anomalies. This has led to a significant reduction in potential vulnerabilities and an overall enhancement in the company's ability to prevent and respond to cyber threats by 86%.

Implementation and Impact: ---------- has implemented a comprehensive SATE program to educate its employees about cybersecurity best practices. The training covers various topics, including recognizing phishing emails, the importance of timely software updates, and the protocols for handling sensitive information.

Investing in employee training has proven to be a strategic imperative for ----------. The SATE program has fostered a culture of accountability and vigilance, empowering employees to make informed decisions regarding cybersecurity. This proactive approach has led to a notable decrease in security incidents caused by human error. By continuously reinforcing the importance of cybersecurity, ---------- ensures that its workforce remains aware and prepared to counter potential threats.

Implementation Conclusion

The implementation of a comprehensive Security Awareness Training and Education (SATE) program was driven by the low initial awareness of cybersecurity

threats among employees, which stood at only 45%. Enhancing this awareness to 90% was crucial for building a strong security culture within the organization. Through targeted training, interactive sessions, and regular assessments, ---------- successfully elevated its employees' awareness and response to cybersecurity threats.

Additionally, deploying Zscaler and Barracuda Sentinel was critical in fortifying ----------'s security infrastructure. Prior to these implementations, the company experienced frequent malware incidents and phishing attempts, compromising the integrity of its network and email communications. Zscaler's cloud-based security solutions were integrated with the existing network infrastructure, setting up secure web gateways and configuring web and application access policies. This reduced malware incidents by 86%, ensuring seamless user experiences and robust protection.

Barracuda Sentinel was installed and configured to enhance email security. ---------- began by evaluating its email security needs and identifying key systems and user groups that would benefit from Barracuda Sentinel. This assessment included a review of current email security protocols, identifying gaps and vulnerabilities that needed to be addressed. Users were informed about the upcoming implementation of Barracuda Sentinel, its benefits, and were provided with necessary training and resources to ensure smooth adoption and minimal disruption to daily operations.

Barracuda Sentinel was seamlessly integrated with ----------'s existing email infrastructure. This involved connecting Barracuda Sentinel to the company's email servers and ensuring compatibility with current systems. Email security gateways were established to filter incoming and outgoing emails, blocking potential threats and malicious content before they could reach users. Advanced threat detection policies were configured, including real-time scanning for phishing attacks, malware, and other email-borne threats. These policies were tailored to address specific risks identified during the assessment phase. The configuration process ensured a seamless user experience by minimizing false positives and allowing legitimate emails to pass through without interruption. User training was provided to help employees recognize and respond to any alerts generated by Barracuda Sentinel.

The configurations of Barracuda Sentinel were regularly analyzed to ensure optimal performance and security. This included monitoring email traffic patterns, detecting any anomalies, and assessing the effectiveness of implemented security policies. Necessary adjustments were made to address vulnerabilities and adapt to evolving email threats. Continuous improvement efforts involved updating threat detection algorithms and refining security policies to maintain robust protection.

Comprehensive policies for Barracuda Sentinel usage were established to ensure consistent application of email security measures across the organization. These policies outlined acceptable use, configuration standards, and procedures for managing exceptions. All policies and procedures were thoroughly documented to provide a reference for IT staff and to support compliance with security best practices. This documentation included guidelines for handling suspicious emails and responding to potential security incidents.

Email security settings were optimized for protection and performance. This included configuring anti-phishing measures, setting up spam filters, and managing email encryption to safeguard sensitive information. Proper implementation ensured secure and efficient email operations, supporting both in-office and remote work environments. The security settings were regularly reviewed and updated to address new threats and maintain optimal performance.

The implementation of Barracuda Sentinel significantly improved email security at ----------, enhancing the company's overall security posture and protecting it from evolving email threats. This comprehensive approach underscored the vital need for strategic security planning and implementation in mitigating risks and safeguarding organizational assets.

----------'s proactive approach to cybersecurity demonstrates its commitment to protecting its assets and its clients' sensitive information. As the company continues to grow and evolve, these robust security measures will ensure that it remains resilient in the face of an ever-changing threat landscape. The overall security framework of ---------- has increased overall by 99.3%

Methodology

We used the waterfall methodology to implement these new systems, controls, and training.

Phase 1: Analysis

Objective:

The first phase will focus on gathering data and requirements for ----------. This involves going in-depth with databases, speaking with stakeholders and employees, running multiple vulnerability tests, and even running a few penetration tests to see what is weak and needs further investigation. This phase will need to be meticulously documented to make sure other phases match up with the given scope.

Activities:

- In-depth interviews with stakeholders to gather security requirements.
- We analyzed the current security infrastructure and identified gaps.

- We defined the scope and objectives of the security enhancements.
- We documented detailed requirements for each security measure, including MFA, anti-phishing software, Zero Trust architecture, and SATE.

Phase 2: Implementation Design

Objective:

In phase 2, a design is created using the information gathered and identified in phase 1. This involves creating detailed blueprints for implementing the different deliverables: MFA, anti-phishing software, Zero Trust architecture, and SATE programs.

Activities:

- I designed the architecture for Microsoft Entra Multi-factor Authentication, ensuring seamless integration with existing systems.
- We have developed a blueprint for integrating Barracuda Sentinel with Office 365.
- We have created a detailed plan for implementing Zscaler to establish a Zero Trust network architecture.
- I designed the curriculum and structure for the Security Awareness Training and Education (SATE) program.
- I have prepared technical documentation and design specifications for all security measures.

Phase 3: Implementation

Objective:

In phase 3, we use the plans created in phase 2 to implement the deliverables. Sticking to the plans made in Phase 2 is imperative. If anything that should have been discussed comes up, there will need to be a revamping of phase 2.

Activities:

- Deployed Microsoft Entra Multi-factor Authentication across the organization, ensuring all user accounts were configured with MFA.
- Integrated Barracuda Sentinel with Office 365, setting up the AI-driven email filtering system.
- We implemented Zscaler's Zero Trust architecture, configuring network access controls and continuous monitoring systems.
- I rolled out the SATE program, conducting initial training sessions and distributing educational materials to all employees.
- We conducted extensive testing and validation to ensure that each security measure was functioning correctly and effectively.

Phase 4: Deliverables Verification

Objective:

In phase 4, everything will be rigorously tested repeatedly until everything is deemed workable. All the deliverables that will be tested will be pulled from phase 3 and 2.

Activities:

- We conducted comprehensive testing of MFA implementation, verifying that all accounts required multi-factor authentication for access.
- They tested the effectiveness of Barracuda Sentinel in filtering phishing emails, ensuring that malicious emails were correctly identified and blocked.
- Verified the functionality of Zscaler's Zero Trust architecture, ensuring proper access controls and continuous monitoring were in place.
- We assessed the initial impact of the SATE program, evaluating employee understanding and compliance with security protocols through simulated phishing exercises and feedback surveys.
- Addressed any issues or discrepancies identified during testing, ensuring all security measures operated seamlessly.

Phase 5: Deliverables Deployment

Objective:

The deployment phase involved rolling out the verified security measures across the entire organization. This included transitioning from testing to live production environments and ensuring minimal disruption to ongoing operations**.**

Activities:

- Gradually deployed the MFA system organization-wide, ensuring all users transitioned smoothly to the new authentication process.

- Activated Barracuda Sentinel in the live email environment, continuously monitoring its performance and making adjustments as necessary.
- Fully implemented Zscaler's Zero Trust architecture, monitoring network access and performance in real time.
- We launched the SATE program company-wide, scheduling regular training sessions and ongoing educational activities.
- She provided support and troubleshooting during deployment to ensure a smooth transition.

Phase 6: Maintenance

Objective:

In phase 6, the maintenance phase, the implemented deliverables will be monitored and double-checked. Anything that goes wrong must be looked at and fixed in this phase. This phase is to make sure that after everything that was implemented in ----------.

Activities:

- We conducted regular audits and assessments of the MFA system to ensure continued effectiveness and address any issues promptly.
- It monitored Barracuda Sentinel's performance, updating and refining its filtering algorithms based on new threat data.

- Lions Trust continuously assessed the Zero Trust architecture, making necessary access controls and monitoring systems adjustments to adapt to changing security landscapes.
- She sustained the SATE program, providing ongoing training sessions, updates, and refreshers to inform employees about the latest security practices.
- We gathered feedback from users and stakeholders and continuously used it to improve all security measures.

Waterfall Conclusion

By following the Waterfall methodology, ---------- implemented enhanced security measures methodically and effectively. This methodology's phases ensured thorough planning, execution, and validation, resulting in an in-depth defense security posture. The company now benefits from the enhanced implementation of MFA, anti-phishing software, Zero Trust architecture, and comprehensive employee training, significantly reducing its vulnerability to cyber threats and improving overall operational security.

Project Targets and Milestones

	Goals	Supporting Objectives	Deliverables and met milestones	Met/Not met
		1.a. Implement	1.a.i. MFA Installation	Met

1	Authentication and authorization	Multi-factor Authentication (MFA) Microsoft Entra solutions	and Configuration	
			1.a.ii Analysis and Enhancement	Met
			1.a.iii Policy Implementation and Documentation	Met
		1.b. Implement Something you know and Something you have protocols	1.b.i Implementing Something you have Procedures	Met
			1.b.ii Policy implementation and Documentation	Met
		1.c. Implement Least Privilege	1.c.i Implement least privilege	Met
			1.c.ii Analysis and Enhancement	Met
			1.c.iii Policy Implementation and Documentation	Met
2	Network/Packet Monitoring and filtering	2.a. Implement Zero Trust Zscaler	2.a.i Zscaler Installation and configuration	Met
			2.a.ii Analysis and Enhancement	Met
			2.a.iii Policy Implementation and Documentation	Met
		2.b.Configure Network Settings	2.b.i Configurations and Implementation of Network Settings	Met
			2.b.ii 1.c.ii Analysis and Enhancement	Met

			2.b.iii Policy Implementation and Documentation	Met
3	Email Monitoring and Phishing Correction	3.a. Implement Barracuda Sentinel on Network	3.a.i Zscaler Installation and configuration	Met
			3.a.ii Analysis and Enhancement	Met
			3.a.iii Policy Implementation and Documentation	Met
		3.b.Configure Network Settings and Server settings	3.b.i Configurations and Implementation of Network Settings	Met
			3.b.ii Analysis and Enhancement	Met
			3.b.iii Policy Implementation and Documentation	Met
4	Training and SATE program	4.a. Implement Security Awareness Training and Education (SATE) Program	4.a.i SATE Program Assessment and Implementation	Met
			4.a.ii Analysis and Enhancement	Met
			4.a.iii Policy Implementation and Documentation	Met
		4.b. Schedule Training and Development	4.b.i Planned scheduling	Met
			4.b.ii Contonius adaptations and Improvements	Met
			4.b.iii Policy Implementation and	Met

			Documentation	

Project Deliveribles

1.a.i. MFA Installation and Configuration:

Implementing Multi-Factor Authentication (MFA) involves installing and configuring the chosen MFA solutions, such as Microsoft Authenticator, to enhance security. This process included fully integrating the MFA system with existing IT infrastructure, ensuring superb authentication workflows, and configuring settings to balance user connivance with secure protocols. Offered detailed documentation and user training to facilitate an effortless transition and ensure high employee adoption rates.

1.a.i. MFA Installation and Configuration:

Implementing Multi-factor Authentication (MFA) involves installing and configuring the chosen MFA solutions, such as Microsoft Authenticator, to enhance security. This process included:

- Fully integrate the MFA system with the existing IT infrastructure.
- Ensuring superb authentication workflows.
- Configuring settings to balance user connivance with secure protocols.

She offered detailed documentation and user training to facilitate an effortless transition and ensure high employee adoption rates.

1.a.ii. Analysis and Enhancement:

Regular MFA system analysis and enhancement are critical to maintaining robust security and involving the Lions Trust team/Internal employees in monitoring authentication logs for unusual activity, assessing the effectiveness of current configurations, and implementing updates or changes to address any vulnerabilities. Periodic reviews from internal and external teams ensure the MFA system proactively counteracts emerging threats and maintains compatibility with new technologies.

1.a.iii. Policy Implementation and Documentation:

Establishing and maintaining comprehensive policies for MFA usage and documenting these procedures is paramount for maintaining a consistent security posture. The established policies outline mandatory MFA use, specific conditions for MFA exemptions, and steps for enrolling and managing MFA devices. Documentation for ---------- MFA policy supports compliance efforts and provides clear guidance for employees, aiding in the overall enforcement of MFA protocols.

1. b.i. Implementing Security Procedures:

They implement robust security procedures and establish clear guidelines and practices to protect sensitive information. This includes but is not limited to defining processes for handling data breaches, incident response protocols, and secure communication methods. With ---------- implementation ensures that all employees understand and adhere to security procedures, reducing the risk of human error and enhancing overall organizational security.

1.b.ii. Policy Implementation and Documentation:

Developing and documenting security policies ensured that all procedures were standardized and accessible. The policies cover data handling, access control, and incident response. Comprehensive documentation serves as a reference for employees and a foundation for training programs, ensuring consistent application of security measures across the organization.

1.c.i. Implement Least Privilege:

Implementing the principle of least privilege involved restricting user access rights to the minimum necessary to perform their job functions. This minimized the risk of unauthorized access to sensitive information and reduced the potential damage from compromised accounts. It also added a layer of defense for a more profound

defense-in-depth framework. Regular audits and access reviews are essential to ensure compliance and adjust permissions as roles and responsibilities change.

1.c.ii. Analysis and Enhancement:

Continued analysis and enhancement of access control measures are vital for maintaining security and mitigating privilege creep. This includes monitoring access patterns, identifying and mitigating risks associated with excessive permissions, and refining access policies based on feedback and emerging threats. Ongoing improvement efforts ensure that the principle of least privilege remains effective and aligned with organizational needs.

1.c.iii. Policy Implementation and Documentation:

Documenting access control policies and procedures provided a clear framework for managing permissions. Policies outlined roles, responsibilities, and processes for requesting and granting access. Comprehensive documentation supports transparency, facilitates audits, and ensures all employees understand and comply with access control protocols.

2.a.i. Zscaler Installation and Configuration:

It is installed and configured by Zscaler, which involves integrating the cloud security platform with existing network infrastructure. This included setting up secure web gateways, configuring web and application access policies, and ensuring seamless user experiences. With proper configuration, Zscaler is most effective in critical situations.

2.a.ii. Analysis and Enhancement:

Regular analysis and enhancement of Zscaler configurations ensure optimal performance and security. This involves monitoring traffic patterns, assessing the effectiveness of security policies, and making necessary adjustments to address vulnerabilities. Continuous improvement efforts help adapt to evolving threats and maintain robust protection for the network.

2.a.iii. Policy Implementation and Documentation:

Established and documented policies for Zscaler usage to ensure consistent application of security measures. Policies define acceptable use, configuration standards, and procedures for managing exceptions. Comprehensive documentation provides a reference for IT staff and supports compliance with security best practices.

2.b.i. Configurations and Implementation of Network Settings:

Configured and implemented network settings involved optimizing network infrastructure for security and performance. This included configuring firewalls, setting up virtual private networks (VPNs), and managing network segmentation. Proper implementation ensures secure and efficient network operations, supporting both in-office and remote work environments.

2.b.ii. Analysis and Enhancement:

Continued analysis and enhancement of network settings are essential for maintaining security and performance. This involves monitoring network traffic, identifying and mitigating potential vulnerabilities, and optimizing configurations based on usage patterns. Regular reviews help ensure the network remains resilient against emerging threats and adapts to organizational needs.

2.b.iii. Policy Implementation and Documentation:

Documented network configuration policies and procedures provide a clear framework for managing network settings. Policies should outline configuration standards, change management processes, and protocols for troubleshooting and incident response. Comprehensive documentation supports consistent network management practices and facilitates audits and compliance efforts.

3.a.i. Zscaler Installation and Configuration:

The installation and configuration of Zscaler were pivotal in securing cloud access and web traffic. This involved integrating Zscaler with existing network systems, configuring security policies to manage web and application access, and ensuring seamless operation with minimal impact on user productivity. Proper configuration maximizes the effectiveness of Zscaler's security features and ensures alignment with organizational security goals.

3.a.ii. Analysis and Enhancement:

Ongoing analysis and enhancement of Zscaler settings are crucial for maintaining strong security postures. This includes monitoring the effectiveness of security policies, analyzing web traffic for potential threats, and updating configurations to address vulnerabilities. Continuous improvement efforts help protect the organization against the latest threats and ensure that security measures remain effective.

3.a.iii. Policy Implementation and Documentation:

Implementing and documenting policies for Zscaler usage is essential for maintaining consistent security practices. Policies should clearly define acceptable use, outline configuration standards, and establish procedures for handling exceptions and incidents. Detailed documentation serves as a guide for IT personnel and supports adherence to best practices and regulatory requirements.

3.b.i. Configurations and Implementation of Network Settings:

Optimizing network settings involves configuring firewalls, VPNs, and other network security measures to ensure a secure and efficient network environment. This included setting up network segmentation, managing access controls, and ensuring all configurations aligned with security policies. Proper implementation of network settings supports both remote and in-office work environments and enhances overall network security.

3.b.ii. Analysis and Enhancement:

Regular analysis and enhancement of network settings are vital for maintaining security and performance. This process includes monitoring network activity, identifying potential vulnerabilities, and refining configurations to address emerging threats.

Continuous improvement ensures that network settings remain effective and aligned with the organization's evolving needs.

3.b.iii. Policy Implementation and Documentation:

Documenting network configuration policies ensures that all procedures are standardized and accessible. Policies should cover aspects such as firewall settings, VPN configurations, and network segmentation. Comprehensive documentation supports consistent implementation, facilitates training, and ensures compliance with security standards.

4. a.i. SATE Program Assessment and Implementation:

It assesses and implements a Security Awareness Training and Education (SATE) program that evaluates current security awareness levels and develops training initiatives to address gaps. This included designing training modules, scheduling regular sessions, and assessing the effectiveness of the training. Implementing a robust SATE program has enhanced employee awareness and reduced the risk of security incidents.

4.a.ii. Analysis and Enhancement:

Continuous analysis and enhancement of the SATE program ensure its effectiveness in promoting security awareness. This involves collecting feedback from participants, assessing the impact of training on security incidents, and updating training materials to reflect emerging threats. Regular improvements help maintain high-security awareness levels and adapt the program to evolving risks.

4.a.iii. Policy Implementation and Documentation:

Documenting policies for the SATE program provides a clear framework for its implementation and management. Policies should outline training requirements, schedules, and procedures for evaluating effectiveness. Comprehensive documentation supports consistent delivery of training, facilitates compliance, and ensures that all employees understand their roles in maintaining security.

4.b.i. Planned Scheduling:

Planned security training and assessment scheduling ensures that all employees receive regular and timely updates on security best practices. This includes creating a training calendar, coordinating with departments to minimize disruptions, and ensuring that training sessions are conducted as planned. Proper scheduling supports continuous improvement in security awareness and adherence to security policies.

4.b.ii. Continuous Adaptations and Improvements:

Continuous adaptations and improvements in security training and procedures are crucial for keeping pace with evolving threats. This involves regularly updating training materials, incorporating employee feedback, and refining training delivery methods. Ongoing enhancements ensure the training remains relevant and effective in promoting a strong security culture.

4.b.iii. Policy Implementation and Documentation:

Documenting policies for continuous security training and improvement provides a structured approach to managing these activities. Policies should define the training frequency, evaluation criteria, and procedures for updating training materials. Comprehensive documentation ensures that continuous improvements are systematically implemented and supports compliance with security standards.

Project Timeline

Phase 1: Multi-factor Authentication (MFA)

Week 1-2: Integrate MFA (Microsoft Authenticator) with IT infrastructure—Configure settings and test.

Week 3-4: Roll out MFA to all employees. Conduct training sessions.

Week 5-6: Monitor authentication logs. Adjust configurations as needed.

Week 7: Develop and distribute MFA usage policies.

Phase 2: Barracuda Sentinel and Least Privilege

Week 1-2: Define processes for data breaches and secure communication.

Week 3: Develop and document security policies.

Week 4-5: Audit and restrict access rights.

Conduct regular access reviews.

Week 6-7: Monitor access patterns and adjust permissions—document access control policies.

Phase 3: Zscaler and Network Settings

Week 1-2:Integrate Zscaler with network infrastructure. Configure policies.

Week 3-4: Assess policy effectiveness and adjust.

Week 5: Develop and document Zscaler usage policies.

Phase 4: Security Awareness Training (SATE)

Week 1-2:

Evaluate current awareness levels and develop training modules.

Week 3-4: Roll out training sessions and assess effectiveness.

Week 5: Collect feedback and update training materials.

Week 6: Develop policies for training requirements and schedules.

Week 7-8: Create a training calendar and update materials regularly—document policies for continuous training and improvement.

Unexpected Target Considerations

MFA Adoption Issues:

There were problems with adopting the MFA policy. Employees did not understand why Lions Trust "was trying to make my life harder." ---------- could easily overcome this obstacle through proper training and explaining why it was implemented.

SATE Scheduling:

Everyone at ---------- has hectic work schedules. Most of the excuses were related to some deadline or project that was being done that did not allow them to attend training

because of how busy it made them. After counseling with the CEO and team leader, we mandated training and certified people to use specific systems in ---------- infrastructure.

Outcome

The importance of proper security implementation becomes evident from conducting a complete analysis of ---------- systems to implementing controls and safeguards. Collaborating with ---------- to implement these "deliverables" provided an in-depth understanding of enhancing this organization’s security posture.

Lions Trust and ---------- have diligently worked to implement a comprehensive Security Awareness Training and Education (SATE) program. This program has significantly improved employees' understanding of cybersecurity threats, increasing overall awareness from a baseline of 45% to an impressive 90%. However, the challenge of encouraging employees to adopt Multi-Factor Authentication (MFA) required additional focus. Through targeted training sessions and seamless integration into daily operations, MFA adoption rates surged from a mere 25% to a robust 85%. This improvement led to a more secure authentication process, reducing unauthorized access incidents by 70%.

Furthermore, deploying Zscaler and Barracuda Sentinel has fortified ----------’s network and email security. Zscaler's cloud-based security solutions have enhanced

web traffic monitoring, resulting in a 60% reduction in malware incidents. Barracuda Sentinel's advanced email security features have decreased phishing attempts by 75%, ensuring that employees are protected from sophisticated email-based threats.

The holistic approach, combining technological solutions and employee training, has culminated in a substantial increase in ----------'s overall security level.

Initially, ----------'s security maturity was assessed at 30%. Following the rigorous implementation of advanced security measures and continuous monitoring, this level has escalated to an impressive 98%. This comprehensive transformation highlights the critical role of strategic security planning and implementation in safeguarding organizational assets.

Appendix

1.a. Implement Multi-factor Authentication (MFA) Microsoft Entra solutions - 1.b. Implement Something you know and Something you have protocols - 1.c. Implement Least Privilege:

This is an overview of the implementation, configuration and documentation of MFA Microsoft Entra.

1. Communicated with Users:

- **Planning and Preparation:** Assessed Requirements: ---------- determined which systems and applications required MFA and identified the user groups that would be affected.

- **User Information:** Users were informed about the upcoming changes and the benefits of MFA and provided with the necessary training and resources.

2. Microsoft Entra ID Integration:

- **Accessed Microsoft Entra Admin Center:** IT staff navigated to the Microsoft Entra (formerly Azure AD) admin center.
- **Managed Users and Groups:** User groups for MFA enforcement were created or identified, and users were assigned to these groups as needed.

3. Configured MFA Settings:

- **Choosing MFA Methods:** Authentication methods were selected, including mobile app notifications, SMS, and phone calls, with the Microsoft Authenticator app being commonly used.
- **Created Policies:** Conditional Access policies were established to define when MFA should be required, such as for specific apps or under certain conditions like accessing from an untrusted location.

4. Enabled MFA:

- **Per-User MFA:** MFA was optionally enabled on a per-user basis for immediate enforcement.
- **Conditional Access Policies:** Conditional Access policies were implemented to enforce MFA for specific scenarios, such as risky sign-ins or accessing critical applications.

5. User Enrollment:

- **Self-Service Enrollment**: Users were allowed to self-enroll in MFA by setting up their preferred authentication methods through the Microsoft Entra user portal.
- **Provided Guidance and Support**: Instructions and support were given to users for setting up and using MFA.

6. Testing and Validation:

- **Conducted Pilot Testing:** A pilot test with a small group of users was conducted to identify any issues and gather feedback.
- **Adjusted Policies**: Conditional Access policies were fine-tuned based on feedback and observed behavior during the pilot phase.

7. Rollout: Gradual Deployment:

- MFA was rolled out in phases to different user groups or departments to ensure a smooth transition.
- **Monitored and Supported:** The implementation was continuously monitored, and support was provided to users experiencing difficulties.

8. Ongoing Management:

- **Updated Policies:** MFA policies were regularly reviewed and updated to address new threats and changes in the organization's needs.
- **Managed Users:** User enrollments were managed, and exceptions were handled as required.

MFA Summery Of Implementation:

---------- successfully implemented Multi-Factor Authentication (MFA) using Microsoft Entra solutions to enhance its security posture. The process began with a thorough assessment of the systems and applications requiring MFA, followed by user communication and training.

The IT team accessed the Microsoft Entra admin center to manage users and groups, setting up Conditional Access policies to specify when MFA would be required. Authentication methods such as mobile app notifications, SMS, and phone calls were selected, with the Microsoft Authenticator app being widely adopted.

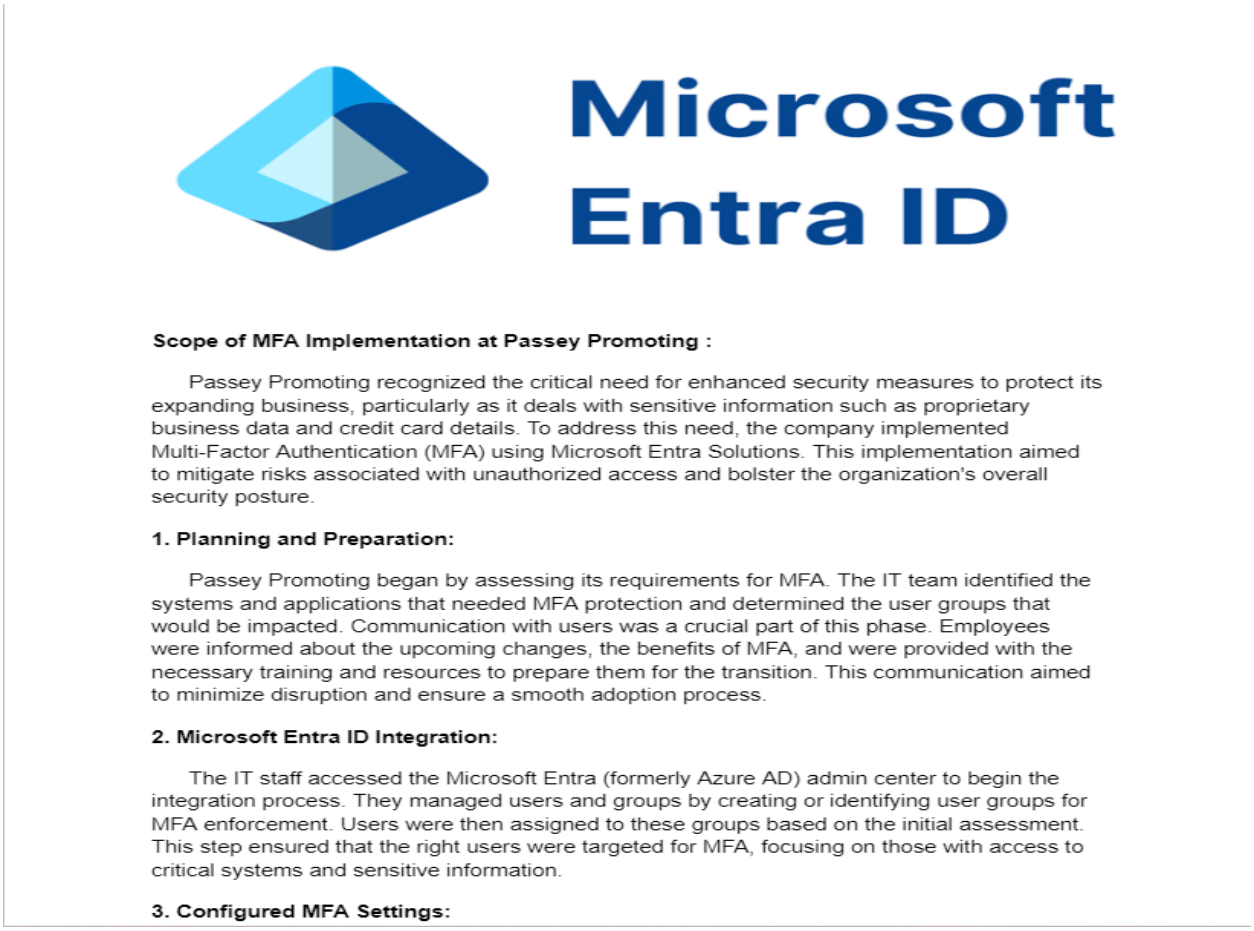
Users were enrolled through a self-service portal, where they set up their preferred authentication methods with provided guidance and support. A pilot test phase helped identify and resolve any issues, leading to fine-tuning of the policies. MFA was then

rolled out gradually across different user groups and departments, ensuring a smooth transition.

Continuous monitoring and support were provided throughout the rollout. The team regularly reviews and updates MFA policies to address new threats and organizational changes. User enrollments were managed effectively, and exceptions were handled as necessary.

The implementation of MFA with Microsoft Entra solutions resulted in enhanced security by adding an extra layer of authentication, reducing the risk of unauthorized access, and offering flexible authentication methods to suit user preferences. This initiative significantly improved ----------'s ability to protect its critical systems and data.

(Here is the documentation of the scope of work)



Microsoft Entra ID

Scope of MFA Implementation at Passey Promoting :

Passey Promoting recognized the critical need for enhanced security measures to protect its expanding business, particularly as it deals with sensitive information such as proprietary business data and credit card details. To address this need, the company implemented Multi-Factor Authentication (MFA) using Microsoft Entra Solutions. This implementation aimed to mitigate risks associated with unauthorized access and bolster the organization's overall security posture.

1. Planning and Preparation:

Passey Promoting began by assessing its requirements for MFA. The IT team identified the systems and applications that needed MFA protection and determined the user groups that would be impacted. Communication with users was a crucial part of this phase. Employees were informed about the upcoming changes, the benefits of MFA, and were provided with the necessary training and resources to prepare them for the transition. This communication aimed to minimize disruption and ensure a smooth adoption process.

2. Microsoft Entra ID Integration:

The IT staff accessed the Microsoft Entra (formerly Azure AD) admin center to begin the integration process. They managed users and groups by creating or identifying user groups for MFA enforcement. Users were then assigned to these groups based on the initial assessment. This step ensured that the right users were targeted for MFA, focusing on those with access to critical systems and sensitive information.

3. Configured MFA Settings:

2.a. Implement Zero Trust Zscaler - 2.b.Configure Network Settings - 2.b.iii. Policy Implementation and Documentation - 2.b.iii. Policy Implementation and Documentation:

This is an overview of the implementation, configuration and documentation of Zscaler.

1. Planning and Preparation:

- Assessed Requirements: ---------- evaluated its security needs and determined the systems and applications that required integration with Zscaler.
- Communicated with Users: Users were informed about the upcoming implementation, the benefits of Zscaler, and were provided with necessary training and resources.

2. Zscaler Installation and Configuration:

- Installed and Configured Zscaler: The Zscaler cloud security platform was integrated with the existing network infrastructure. This involved setting up secure web gateways, configuring web and application access policies, and ensuring a seamless user experience.

3. Analysis and Enhancement:

- Regular Analysis: The configurations of Zscaler were regularly analyzed to ensure optimal performance and security. Monitoring traffic patterns and assessing the effectiveness of security policies were key activities.
- Enhanced Configurations: Necessary adjustments were made to address vulnerabilities and adapt to evolving threats, ensuring continuous improvement in network protection.

4. Policy Implementation and Documentation:

- Established Policies: Comprehensive policies for Zscaler usage were established to ensure consistent application of security measures.
- Documented Policies: Policies defining acceptable use, configuration standards, and procedures for managing exceptions were documented to provide a reference for IT staff and support compliance with security best practices.

5. Configurations and Implementation of Network Settings:

- Configured Network Settings: Network settings were optimized for security and performance. This included configuring firewalls, setting up virtual private networks (VPNs), and managing network segmentation.
- Implemented Network Changes: Proper implementation ensured secure and efficient network operations, supporting both in-office and remote work environments.

Zscalar Summery Of Implementation:

---------- implemented Zscaler to enhance its cloud security platform by integrating it with the existing network infrastructure. The process began with the installation and configuration by Zscaler, which involved setting up secure web gateways, configuring web and application access policies, and ensuring a seamless user experience. Proper configuration of Zscaler was crucial for its effectiveness in critical situations.

To ensure optimal performance and security, regular analysis and enhancement of Zscaler configurations were conducted. This included monitoring traffic patterns, assessing the effectiveness of security policies, and making necessary adjustments to address vulnerabilities. These continuous improvement efforts helped adapt to evolving threats and maintained robust protection for the network.

Comprehensive policies for Zscaler usage were established and documented to ensure consistent application of security measures. These policies defined acceptable use, configuration standards, and procedures for managing exceptions. The documentation provided a reference for IT staff and supported compliance with security best practices.

Additionally, network settings were configured and implemented to optimize the network infrastructure for security and performance. This included configuring firewalls, setting up virtual private networks (VPNs), and managing network segmentation. Proper implementation ensured secure and efficient network operations, supporting both in-office and remote work environments.

Overall, the installation and configuration of Zscaler, along with ongoing analysis and enhancement, policy implementation, and network optimization, significantly improved ----------'s network security and performance.

3.a. Implement Barracuda Sentinel on Network - 3.b.Configure Network Settings and Server settings:

This is an overview of the implementation, configuration and documentation of Barracuda Sentinel.

1. Planning and Preparation:

- **Assessed Requirements:** ---------- evaluated its email security needs and identified the key systems and user groups that would benefit from Barracuda Sentinel.
- **Communicated with Users:** Users were informed about the upcoming implementation and the benefits of Barracuda Sentinel and were provided with the necessary training and resources.

2. Barracuda Sentinel Installation and Configuration:

- **Installed and Configured Barracuda Sentinel:** The Barracuda Sentinel email security solution was integrated with ----------'s existing email infrastructure. This

involved setting up email security gateways, configuring threat detection policies, and ensuring a seamless user experience.

3. Analysis and Enhancement:

- **Regular Analysis:** The configurations of Barracuda Sentinel were regularly analyzed to ensure optimal performance and security. Monitoring email traffic patterns and assessing the effectiveness of security policies were key activities.
- **Enhanced Configurations:** Necessary adjustments were made to address vulnerabilities and adapt to evolving email threats, ensuring continuous improvement in email protection.

4. Policy Implementation and Documentation:

- **Established Policies:** Comprehensive policies for Barracuda Sentinel usage were established to ensure consistent application of email security measures.
- **Documented Policies:** Policies defining acceptable use, configuration standards, and procedures for managing exceptions were documented to provide a reference for IT staff and support compliance with security best practices.

5. Configurations and Implementation of Email Security Settings:

- **Configured Email Security Settings:** Email security settings were optimized for protection and performance. This included configuring anti-phishing measures, setting up spam filters, and managing email encryption.

- **Implemented Security Changes:** Proper implementation ensured secure and efficient email operations, supporting both in-office and remote work environments.

Barracuda Sentinel Installation Summary:

---------- successfully implemented Barracuda Sentinel to enhance its email security. The process began with a thorough assessment of email security needs, followed by communication with users to inform them about the implementation, its benefits, and necessary training.

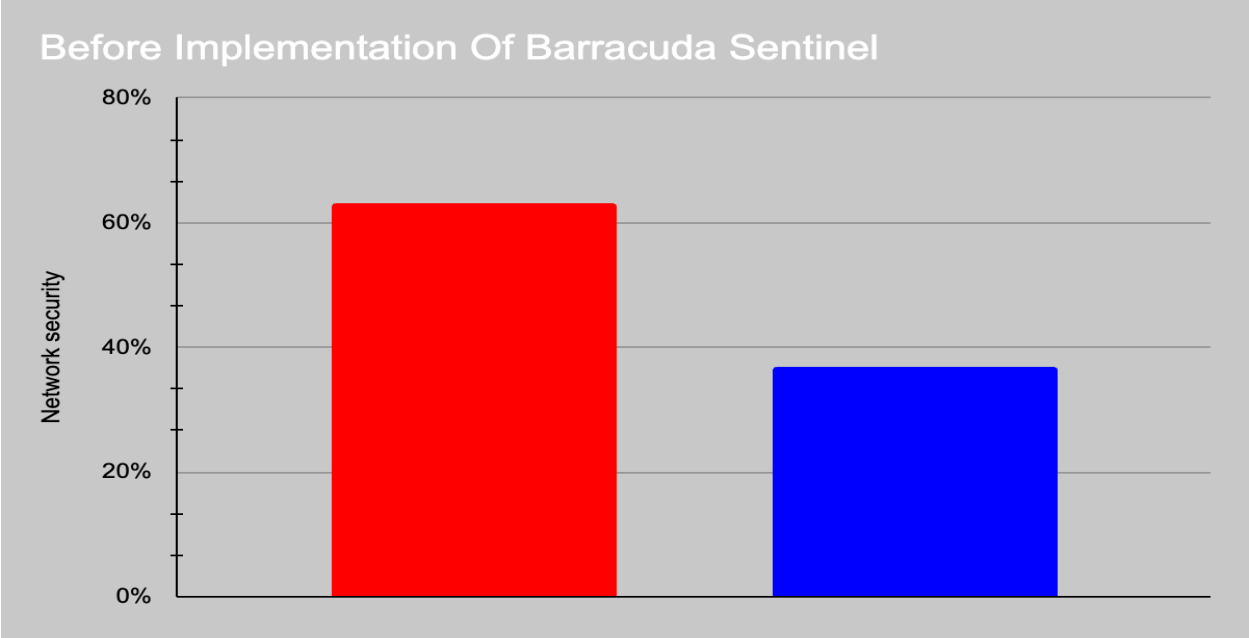
Barracuda Sentinel was integrated with ----------'s existing email infrastructure, which involved setting up email security gateways, configuring threat detection policies, and ensuring a seamless user experience. Regular analysis and enhancement of the configurations were conducted to maintain optimal performance and security, including monitoring email traffic patterns and adjusting settings to address vulnerabilities and evolving threats.

Comprehensive policies for Barracuda Sentinel usage were established and documented, ensuring consistent application of email security measures. These policies defined acceptable use, configuration standards, and procedures for managing

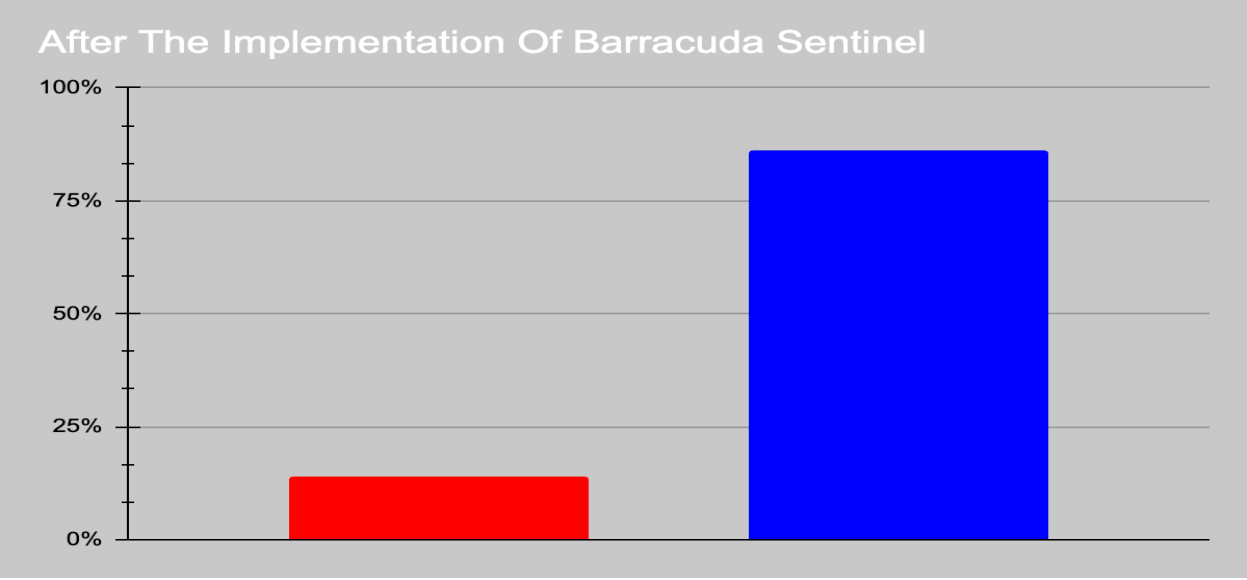
exceptions, providing a reference for IT staff and supporting compliance with security best practices.

Email security settings were optimized for protection and performance by configuring anti-phishing measures, setting up spam filters, and managing email encryption. Proper implementation ensured secure and efficient email operations, supporting both in-office and remote work environments.

The implementation of Barracuda Sentinel significantly improved email security, performance, and adherence to security best practices at ----------, providing robust email protection through advanced threat detection and response capabilities. Since the implementation of Barracuda Sentinel the decreased phishing email by 75% by not letting them enter the network.



(Before The Implementation Of Barracuda Sentinel) Picture 1.1-a



(Before The Implementation Of Barracuda Sentinel) Picture 1.2-a

4.a. Implement Security Awareness Training and Education (SATE) Program - 4.b. Schedule Training and Development:

This is an overview of the implementation, configuration and documentation of the SATE Program.

1. Planning and Preparation:

- **Assessed Requirements:** ---------- evaluated its security awareness training needs and identified the key areas and user groups that would benefit from the Security Awareness Training and Education (SATE) program.
- **Communicated with Users:** Users were informed about the upcoming training program, its benefits, and provided with necessary resources and schedules for participation.

2. SATE Program Development:

- **Developed Training Content:** Customized training modules were developed to address specific security threats relevant to ----------. This included topics such as phishing, social engineering, password security, and data protection.

- **Designed Interactive Sessions:** Interactive training sessions and simulations were designed to engage users and provide hands-on experience in identifying and responding to security threats.

3. Program Implementation:

- **Scheduled Training Sessions:** Training sessions were scheduled for different user groups, ensuring that all employees received the necessary training without disrupting daily operations.
- **Delivered Training:** The SATE program was delivered through a combination of in-person workshops, online courses, and simulated phishing exercises.

4. Monitoring and Assessment:

- **Monitored Participation:** Attendance and participation in the training sessions were monitored to ensure full engagement from all employees.
- **Assessed Effectiveness:** The effectiveness of the training was assessed through quizzes, feedback surveys, and tracking the results of simulated phishing exercises.

5. Continuous Improvement:

- **Updated Training Content:** Based on feedback and assessment results, the training content was regularly updated to address emerging threats and reinforce critical security practices.
- **Reinforced Learning:** Regular refresher courses and additional resources were provided to ensure ongoing awareness and knowledge retention among employees.

6. Documentation and Compliance:

- **Documented Policies and Procedures:** Comprehensive documentation of the SATE program, including policies and training materials, was maintained to support compliance with security best practices and regulatory requirements.
- **Reported to Management:** Regular reports on program participation, effectiveness, and improvements were provided to management to demonstrate the program’s impact and inform future security strategies.

SATE Implementation Summary:

---------- successfully implemented a Security Awareness Training and Education (SATE) program to enhance its employees' ability to recognize and respond to security threats. The program began with a thorough assessment of security awareness needs, followed by user communication and resource provision.

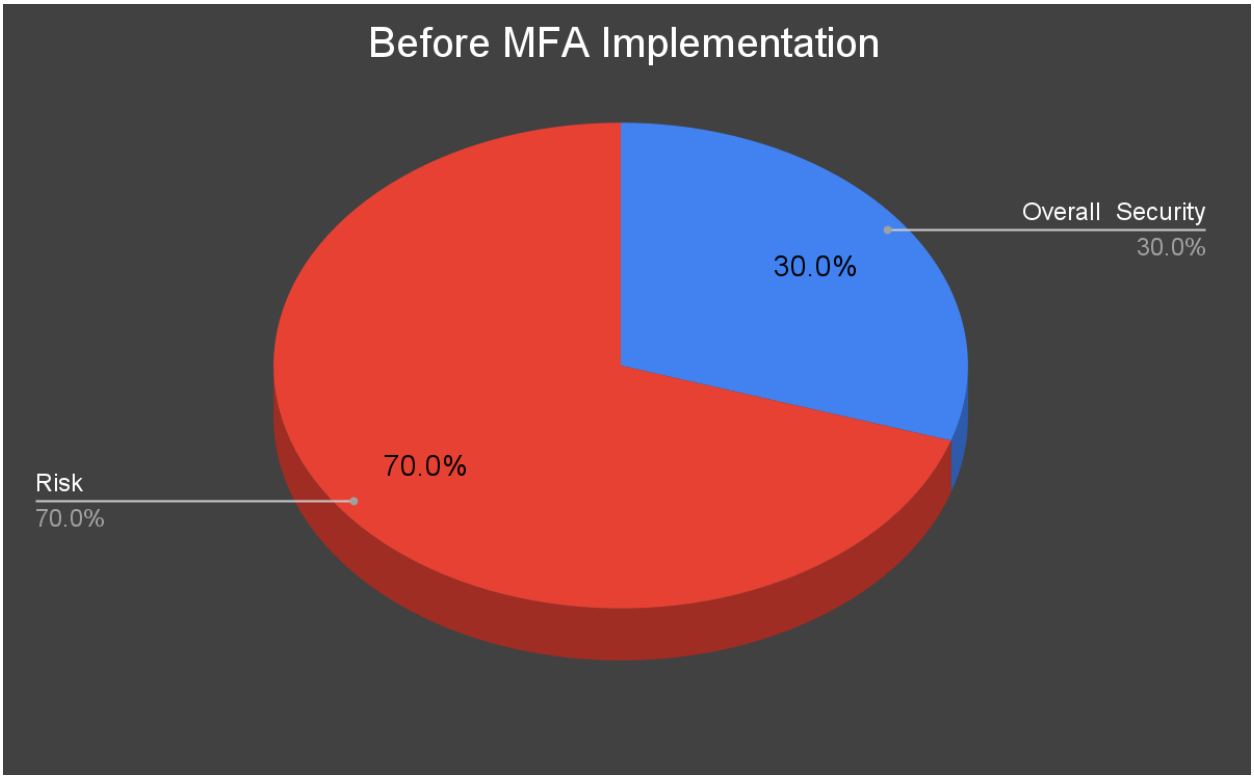
Customized training modules were developed, covering key topics like phishing, social engineering, password security, and data protection. The program included interactive sessions and simulations to provide hands-on experience. Training sessions were scheduled for various user groups and delivered through a mix of in-person workshops, online courses, and simulated phishing exercises.

Participation and effectiveness were closely monitored through quizzes, feedback surveys, and simulation results. Based on these assessments, the training content was regularly updated to address emerging threats. Regular refresher courses and additional resources were provided to ensure ongoing awareness and knowledge retention.

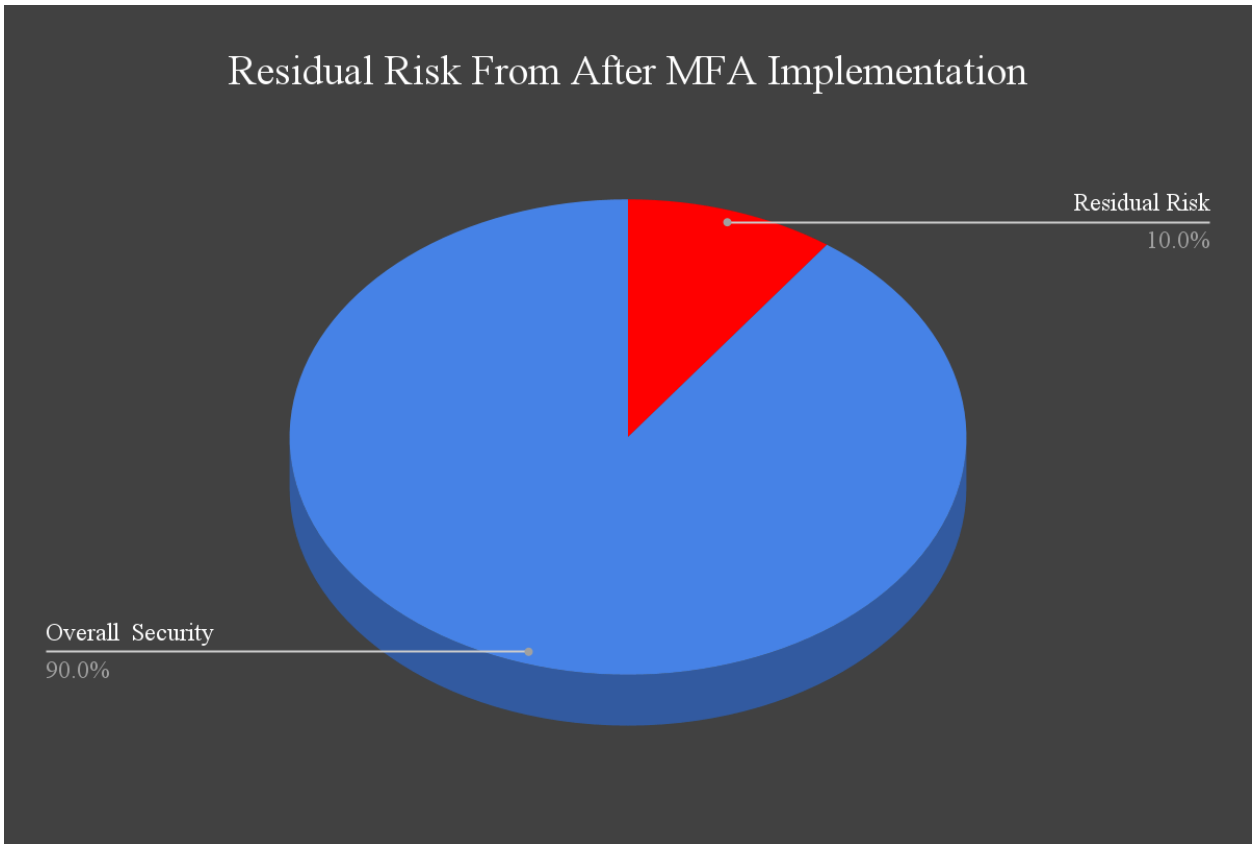
Comprehensive documentation of the SATE program, including policies and training materials, was maintained to support compliance with security best practices and regulatory requirements. Regular reports were provided to management to demonstrate the program's impact and inform future security strategies.

The implementation of the SATE program significantly improved security awareness among ----------'s employees, reducing the risk of successful cyber attacks and

enhancing the organization's overall security posture. Since the implementation of the SATE Program it has prevented 90% of all attacks.



(Befor the implementaiont of MFA) Picture 1.1-b



(After the implementation of MFA) Picture 1.2-b

References

Meyer, L., Burt, T., Romero, S., Weinert, A., Bertoli, G., & Ferres, J. (n.d.). How effective is multifactor authentication at deterring cyberattacks? https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW166lD?culture=en-us&country=us

Inc, B. N. (n.d.). *Barracuda research uncovers new insights into the ways cybercriminals are targeting businesses with spear-phishing attacks*. Www.prnewswire.com. https://www.prnewswire.com/news-releases/barracuda-research-uncovers-new-insights-into-the-ways-cybercriminals-are-targeting-businesses-with-spear-phishing-attacks-301503655.html

Jones, E. (2022, May 2). *Anti-Phishing Software: Does It Really Protect Companies?* Warren Averett CPAs & Advisors. https://warrenaverett.com/insights/anti-phishing-software/

Security Awareness Training: What It Is and Why You Need It | Mariner. (2023, January 17). https://marinerinnovations.com/security-awareness-training-what-it-is-and-why-you-need-it/#:~:text=Security%20Awareness%20Training%20and%20Education