David Garlisch

MSCIA Capstone – D490

Enhancing Security Through Multi-Factor Authentication and Least Privilege

A.  Security Problem

1.  The security problem is the company's failure to implement multi-factor authentication (MFA) and enforce the principle of least privilege within its access controls. Not using MFA when dealing with customers' financial data, which is also personally identifiable information (PII), can be a big problem for the company, not only with their reputation but with regulatory compliance. This issue is particularly critical for the company, which operates as an eCommerce business serving customers worldwide, including those in the European Union (EU). The company will need to comply with PCI-DSS and GDPR. MFA will help them bolster security and achieve these goals. The lack of proper enforcement of least privilege with access controls means that users have more access rights than necessary. This is why we must create a security awareness and training program. In this high-risk environment, where regulatory compliance and data protection are paramount, implementing MFA and least privilege is essential to safeguarding sensitive information and maintaining the trust of the company's customers.

2.  Provide documentation related to the security problem demonstrating the need for a solution, referencing applicable white papers or articles.

The need for the company to implement multi-factor authentication (MFA) and enforce the principle of least privilege is adhered to by several respectable sources. The PCI Security Standards Council states the importance of MFA in securing sensitive information by saying, “The intent of multi-factor authentication (MFA) is to provide a higher degree of assurance of the identity of the individual attempting to access a resource, such as physical location, computing device, network or a database. MFA creates a multi-layered mechanism that an unauthorized user would have to defeat in order to gain access” (PCI Security Standards Council, 2017). This aligns with the company’s need to protect customers' financial data, including personally identifiable information (PII). The Cybersecurity and Infrastructure Security Agency (CISA) highlights the effectiveness of MFA in preventing unauthorized access by noting, “The use of MFA on your accounts makes you 99% less likely to be hacked” (CISA, n.d.). This shows the significant reduction in risk that the company could achieve by implementing MFA, especially in the company’s high-risk environment, where compliance with GDPR and PCI-DSS is mandatory.

The lack of proper enforcement of the least privilege within the company’s access controls increases the risks of insider threats, data breaches, or accidental data exposure. Implementing least privilege is crucial for limiting access to sensitive information, which reduces the potential of unauthorized access. Cybersecurity experts state, "The Principle of Least Privilege directly contributes to data protection by restricting access to confidential and sensitive information. Even if an attacker gains access to a user or system with limited privileges, their ability to exfiltrate critical data remains limited, providing an additional defense against data breaches" (YouAttest, n.d.). This helps highlight the need to implement and enforce the need for least privilege as a core aspect of the company's security strategy.  
  
3. Summarize Problem  
**Not Utilizing Multi-Factor Authentication (MFA):** The company's failure to implement MFA is a crucial root cause of its security vulnerabilities. Relying solely on single-factor authentication leaves the organization susceptible to phishing attacks running rampant throughout the employees' mail inboxes and unauthorized access that can happen because of these types of attacks. This is especially important when handling customers' financial data and personally identifiable information (PII). This lack of MFA not only exposes the company to high-security risks but also creates regulatory compliance gaps with GDPR and PCI-DSS. Both of which mandate strong authentication measures. Without the use of MFA, the company faces an increased risk of data breaches, legal and financial issues, and harm to its reputation.

**Not Utilizing Least Privilege:** The insufficient enforcement of the principle of least privilege within the company's access controls is another major root cause of the security problem. Users are granted more access rights than necessary, which increases the risk of insider threats, accidental data exposure, and unauthorized access. This failure to properly restrict access also highlights gaps in regulatory compliance, as GDPR and PCI-DSS require strict access control measures. Additionally, the company's lack of adequate security awareness and training only worsens the issue, as employees may not understand the importance of least privilege or how to adhere to it, nor how to handle or easily spot phishing attacks. Not utilizing the principle of least privilege only makes the company as a whole more vulnerable to internal and external threats.

B.  **Summarize Stakeholder Role**

**Executive Management -**

* **Implementation Involvement and Needs**:  
  Executive management is responsible for approving the project and then overseeing that the project aligns with the business’s goals while allocating resources accordingly. They will need assurance that the security measures, MFA and least privilege, will reduce these risks, comply with regulatory requirements, and protect the company’s reputation.
* **Impact of the Security Problem**:  
  Security vulnerabilities such as unauthorized access or data breaches could significantly impact the company's finances, lead to regulatory fines, and damage customer trust. The company's strategic goals will be hindered if these security issues are not addressed.
* **Influence on the Objectives and Outcomes**:  
  Their influence ensures that the project receives the necessary support, and their approval is crucial to moving the project forward because executive management is the ones who set the goals and priorities for the project.

**IT Security Team -**

* **Implementation Involvement and Needs**:  
  The IT security team will take care of the technical deployment of MFA and enforce the principle of least privilege with access controls throughout the company. They will need access to the necessary tools, a clear understanding of policies, and continuous, ongoing training to ensure the solution set by executive management is implemented effectively. Additionally, they require ongoing monitoring capabilities to maintain and adjust the system after implementation.
* **Impact of the Security Problem**:  
  The IT security team is responsible for mitigating security risks. Failure to implement MFA and least privilege will place a heavier burden on the team to respond to security incidents, manage breaches, and keep systems secure, which can prove to be overwhelming without the use of proper controls.
* **Influence on the Objectives and Outcomes**:  
  The IT security team provides expertise in how the project is designed and implemented. Because they are at the forefront of these issues with mitigating risks and talking to users, their feedback on risks, system compatibility, and security measures will shape the technical success of the project. They also can help ensure the project’s objectives are realistic and achievable from a security perspective.

**End-Users/Employees -**

* **Implementation Involvement and Needs**:  
  Employees must adopt the use of MFA and adhere to new access control policies set by executive management, which will involve initial training and ongoing support by the IT team. Their needs include easy-to-use MFA tools, clear communication on the changes, and an understanding of the importance of following least privilege policies. We can also review the importance of compliance with PCI-DSS/GDPR, which is paramount to the project's success.
* **Impact of the Security Problem**:  
  Employees are at risk of being targeted by phishing attacks, especially without MFA, which could result in unauthorized access to sensitive data. Additionally, employees may unknowingly have excessive access to critical systems, which increases the risk of accidental data exposure or insider threats. Not following compliance guidelines for handling customer financial data, PII, or utilizing MFA can result in widespread security issues throughout the company.
* **Influence on the Objectives and Outcomes**:  
  User adoption is critical to the success of the project. If employees fail to follow MFA protocols, misunderstand least privilege policies, and do not comply with PCI-DSS and GDPR regulations, the project's effectiveness will be compromised. Their feedback during the security awareness training and implementation phases will help adjust the approach to make the rollout more efficient and effective.

**Compliance Officers** -

* **Implementation Involvement and Needs**:  
  Compliance officers will oversee the project to ensure it meets legal and regulatory standards, specifically regarding GDPR and PCI-DSS. They will use detailed documentation, audit trails, and reporting mechanisms to verify that all implemented controls comply with PCI-DSS and GDPR laws.
* **Impact of the Security Problem**:  
  Non-compliance with regulations can result in costly fines, legal repercussions, and damage to the company’s reputation and even operation. The security issues also make it difficult for compliance officers to ensure that the company’s data handling practices meet the rigorous requirements set by GDPR and PCI-DSS.
* **Influence on the Objectives and Outcomes**:  
  Compliance officers significantly influence the project's success by defining the regulatory objectives that need to be met. They will guide the project to ensure that the solution addresses security risks and also fulfills audit and compliance standards. Their sign-off is essential for project completion.

C.  **Historical data used to support decision-making**

**Historical Data -**

* **Audit and Compliance Review**:  
  Internal and external audits and a previous compliance review revealed significant gaps in the company’s security posture, particularly regarding GDPR and PCI-DSS requirements. These findings highlighted non-compliance in access control and data protection, including the lack of MFA and excessive user permissions. Audit and regulatory reviews flagged these issues as critical risks that could lead to data breaches and significant fines, which further reinforces the need for MFA and least privilege enforcement to meet these compliance standards.
* **Incident Reports and Breach Analysis**:  
  Historical data from security incidents, including unauthorized access attempts and phishing attacks, provided further evidence of the company’s vulnerabilities. Several incidents occurred where attackers accessed sensitive data using compromised employee credentials. These breach reports highlighted the critical need for MFA to reduce the likelihood of such attacks. Additionally, some incidents involved misuse of privileges by internal users, emphasizing the importance of implementing least privilege.
* **Employee Training Feedback**:  
  Previous attempts to raise awareness about security policies showed a lack of employee understanding of best data protection and access control practices. We found that employees frequently reported difficulty in understanding the importance of restricting access and implementing stronger authentication measures, which influenced the decision to create a more structured security awareness training program alongside the use of technical controls.
* **Vulnerability Scans and Penetration Testing**:  
  Vulnerability scans and penetration tests identified multiple security weaknesses, including exposed credentials, unpatched software, and weak access controls. These tests revealed several entry points that attackers could exploit, especially due to the lack of MFA and excessive user permissions left over from privilege creep or permissions given that the user simply doesn’t need to perform their job function. This highlights the need for stronger authentication mechanisms and for the company to utilize the principle of least privilege to mitigate risks from both external and internal threats.

D.  **Project Requirements**

1.  **Industry-Standard Methodologies:** This project will follow guidelines from NIST Cybersecurity Framework and ISO/IEC 27001 standards. These are both some of the gold standards for maintaining a secure environment and it offers many ways to protect PII and help ensure compliance with PCI-DSS and GDPR.

**Requirements:**

* **MFA:** MFA must be implemented across all systems that handle sensitive data and PII. This system must allow for the tracking and auditing of users access attempts to comply with GDPR and PCI-DSS
* **Least Privilege using RBAC:** Microsoft Azure is what we will use for our RBAC system. It must ensure that all users only have access to perform their job function, meaning no excess privileges across any account. The system must allow for automated adjustments for the roles we assign each user to use RBACs. The IT team must be able to continuously monitor these permissions and controls to ensure the least privilege policy is enforced. Also, we must ensure that we can provide detailed logging for audits to comply with GDPR and PCI-DSS.
* **Stakeholder Requirements:**
  + **Executive Management:** The solution must address the company's regulatory concerns by delivering a solution that complies with GDPR and PCI-DSS.
  + **IT Team:** The IT security team will need the appropriate tools to implement the needed changes of the project and also be able to track and monitor access controls. We can have the team use SolarWinds to audit and monitor.
  + **Employees:** To ensure employees adopt these changes with relative ease so there is no hidden delays on the project timeline, there must be clear communication and training provided to them on the new policies, importance, and use of MFA, why least privilege is being enforced, and the importance of compliance with GDPR and PCI-DSS, as well as how to handle and spot phishing attacks.
  + **Compliance Officers:** The solution must have logs for the compliance officers to audit to ensure compliance with PCI-DSS and GDPR. We will need the ability for the compliance officers to track this in real-time.
* **Regulatory Compliance**
  + **NIST Cybersecurity Framework:** Will help implement MFA and least privilege, which are both critical to the project's success. It will also offer guidance to ensure compliance with GDPR and PCI-DSS.
  + **ISO/IEC 27001:** Will guide the project design and development of an Information Security Management System (ISMS). This system will help enforce policies such as the principle of least privilege and support MFA use. ISMS will help maintain and improve security for the company over time.

2. **Launch and Phases**

In this project, the Agile Framework would work best because it allows for iterative development and feedback throughout the project lifecycle and phases, which will be crucial for ensuring compliance and the education of our employees to meet our project goals successfully. Using the Agile framework methodology ensures that any issues encountered during each phase are adequately addressed and that the project remains flexible to any changes that may occur.

* **Phase 1 (Month 1):** This is where the IT team should identify current gaps in access controls: finding any weaknesses in the authentication process for users. We will conduct an audit of our permissions and get a better understanding of where and how to implement MFA and least privilege.
* **Phase 2 (Month 2-3):** Now the project will start deploying MFA for any identified high-risk systems in the company to help with insider threats and overall bolster security for those critical systems. We will identify these systems by which ones handle the most sensitive data in the company or which one’s house PII.
* **Phase 3 (Month 4-5):** In this phase we can implement the principle of least privilege. We can focus on assigning the least amount of permissions required for the users to perform there jobs. We can start with the critical systems and we identified previously. We can utilize Role-based Access Controls, which will work perfectly with our goals for least privilege. We can then easily put people into certain groups going forward when the accounts are created, which will automatically assign each users there roles and mitigate privilege creep.
* **Phase 4 (Month 6):** The project will have the IT team create a security training and awareness program for all users that will be mandatory at least once a year and for all new hires. Users will be educated on the importance of MFA, least privilege, phishing attacks, and compliance with PCI-DSS and GDPR. We can also show the users how to securely manage their credentials and how to comply with all these new changes taking in feedback and continuing education with users if any of our IT teams “phishing attack” emails get through to them. The IT team will also rollout our new newsletter that helps remind users of the importance of all we stated in the meeting and to keep them up-to-date and informed on such topics.
* **Phase 5 (Month 7-8):** At month 7 we can start deploying MFA and least privilege to all of the remaining systems left throughout the organization. While ensuring user acceptance and compliance with these tools and access controls.
* **Phase 6 (Month 9):** For the last month the project will conclude the implementation by conducting a final review while continuously monitoring everything we have implemented. We can track the effectiveness of the project and have one last audit to ensure compliance is achieved, while having time to adjust any access controls. We will utilize feedback and test rigorously before concluding the project and make sure to meet all project markers.

3.  **Implementation Risks**

* **User Acceptance/Resistance to the changes (High Likelihood ):** Users may have a hard time adapting to the new changes. These changes can add newly found stress to their daily workflow. If the users are unwilling to make these changes or training is unclear and doesn’t highlight the importance of adopting these changes, it can cause the project to delay greatly or fail. We will need to make sure our IT team who will create the security training and awareness program also takes time outside of that program to help address and alleviate any concerns users may have to ensure an easier adoption period.
* **Compatibility Issues (Moderate Likelihood):** The company could have some legacy systems that give us a hard time until we find compensating controls or can fully adapt the systems to the proper modern changes. This can delay or add financial impact to the project. Identifying these systems quickly to ensure we can use MFA and RBAC’s to them will be crucial making sure we can properly follow the project timeline with the given budget.
* **Project Delay and Constraints (Moderate Likelihood):** Budgetary constraints, possible limited availability of staff, or possible competing priorities that may come up for the company could lead to delays or financial problems. Having insufficient resources or a big enough budget within the given timeframe could also hinder the continuous monitoring after the rollout of the project. Proper resource allocation and project management will be paramount to a successful project, keeping it on track and in the project timeline.

E.  Training Program

**Audience:** The training program will target all of the company’s users and will focus on general employees who must adopt MFA and follow least privilege policies, the IT security team, who will be responsible for implementing and monitoring these controls, and executive management along with the compliance officers overseeing the alignment with business goals and regulations. Any and all new hires will be integrated into the program during their onboarding process to ensure they are aware of the security measures from the start.

**Delivery:** The training will be delivered through a mix of in-person workshops or online webinars for remote employees. We will also create self-paced online training modules, monthly security newsletters to keep users informed, and IT will create phishing email simulations to help educate any users who do not properly handle them. The online and in-person sessions will cover the importance of MFA, least privilege, how to handle phishing attacks, password policies, and how to properly comply with PCI-DSS and GDPR. The newsletters will keep employees updated on security initiatives, and phishing attack simulations will help reinforce awareness, along with some tailored feedback provided to those who fall for the simulated attacks. New hires will receive the same training upon being hired.

**Content:** For most employees, the training will focus on the importance of MFA, the principle of least privilege, phishing attack awareness, and complying with PCI-DSS and GDPR. The IT security team will receive advanced training on deploying and monitoring MFA and access control systems, as well as managing phishing simulations and the security part of the newsletter. Executive management and compliance officers will receive high-level overviews of how these security measures support regulatory compliance and business goals.

**Duration:** The training program will roll out over four weeks. General employees and any new hires, will attend a 2-hour live session, followed by an hour of self-paced online training. The IT security team will have a full work week of a workshop that focuses on implementing MFA and least privilege. Along with the other things being implemented in the project as they will have to help users and create the newsletters. Executive management/compliance officers will attend a 1-hour briefing. Phishing simulations and newsletters will be ongoing to help maintain a secure environment along with informed and educated users.

F.  **Project/Phase Cost**

**Phase 1 Access Controls:**

* **Resources:** We will need a security tool for conducting audits of access controls, such as a access management analysis tool
* **Cost:** SolarWinds will suit our needs and audit for $1200(SolarWinds, n.d.).

**Phase 2 MFA:**

* **Resources:** We will need an MFA software such as Microsoft Azure
* **Cost:** Microsoft Azure has pricing for Microsoft Entra ID P1 that has MFA and RBAC for $6 per user, totaling around $1800 a month for our 300 employees, which is $21,600 annually (Microsoft, n.d.).

**Phase 3 Least Privilege (RBAC):**

* **Resources:** The company can use Microsoft Azure as we used in Phase 2, which helps us bundle and save money. Phase 2 and 3 are a total of $1800 combined.
* **Cost:** We will sue Microsoft Azure, Microsoft Entra ID P1 is for RBAC as well as MFA which we already priced at $21,600 annually (Microsoft, n.d.)

**Phase 4 User Training and Awareness:**

* **Resources:** For our training program we will create everything in house and that is tailored to our specific needs and goals. We can use Articulate 360, which is a well-known creation tool for training programs. We can then use Cofense’s PhishMe security awareness with risk validation (Cofense, n.d.). Lastly, for our remote employee’s and for convenience sake, we will need an online platform to host webinars. We will use Zoom (Zoom, n.d.).
* **Cost:** The cost for 1 of our IT team members to help create the training program using Articulate 360 is $1499 (Articulate 360, n.d.). We only need one login because the team can still collaborate as the plan allows for that. The cost for the phishing attack simulation is $10 per user, which will total $3,000 annually. We can use it one year and assess from there. We then can price in Zoom where we can have up to 300 participants per webinar at the cost of $18 per user. We know this is not for everyone of our employees, so we will say this is around $2000. This phase will total $6500. This is expensive compared to other phases, but proper training of employees will be itself back 10-fold.

**Phase 5 Rollout of MFA and Least Privilege enforcement:**

* **Resources:** The resources used will be SolarWinds to continuously monitor and audit, while Microsoft Azure helps with MFA and least privilege. These prices are already taken into account and are within the first three phases.
* **Cost: $0.00**

**Phase 6 Continuous Monitoring and Final Review:**

* Resources: SolarWinds will be used for continuously monitoring and auditing, removing the need for any additional cost. SolarWinds can also be used to make sure we achieve compliance with PCI-DSS and GDPR
* **Cost:** $0.00

**Estimated Total Project Cost:** $29,300

**G.**   **Project Deliverables**

The final project deliverables start with a comprehensive audit report that identifies deficiencies in access controls, permissions, and any possible authentication issues. Multi-Factor Authentication (MFA) will be implemented initially for high-risk systems, with detailed policy documentation and user guides for employees. Role-Based Access Controls will be utilized to enforce the principle of least privilege, supported by both compliance documentation and audit logs. A complete security awareness and training program will be created and provided to employees, which will cover key areas such as MFA, least privilege, phishing attack prevention, and the importance of regulatory compliance with GDPR and PCI-DSS. Continuous monitoring of our newly added MFA and access control systems will be implemented, along with final audit reports to ensure we achieve compliance with them. This will be reinforced through ongoing user education through our security section in our newsletters sent out to all employees. Refresher courses and continued education will be available to users who continue to not adhere to new policies and to maintain awareness and security best practices.

G1. **Access Controls Audit and Gap Analysis (Duration: 1 Month):**

* **Start Date**: January 1st, 2025 (Month 1)
* **End Date**: January 31st, 2025 (Month 1)
* **Resources**: IT Security Team, SolarWinds
* **Deliverable**: Audit report that effectively identifies access control gaps in the existing systems

**MFA Deployment for High-Risk Systems (Duration: 2 Months):**

* **Start Date**: February 1st, 2025 (Month 2)
* **End Date**: March 31st, 2025 (Month 3)
* **Resources**: IT Security Team, Microsoft Azure Entra P1
* **Deliverable**: MFA implemented for all critical systems handling sensitive data

**Least Privilege Implementation via RBAC (Duration: 2 Months):**

* **Start Date**: April 1st, 2025 (Month 4)
* **End Date**: May 31st, 2025 (Month 5)
* **Resources**: IT Security Team, Microsoft Azure for RBAC
* **Deliverable**: RBAC will be fully implemented for critical systems, with user permissions strictly aligned to their roles to allow for least privilege

**Security Training and Awareness Rollout (Duration: 1 Month):**

* **Start Date**: June 1st, 2025 (Month 6)
* **End Date**: June 30th, 2025 (Month 6)
* **Resources**: IT Security Team, Cofense PhishMe , Articulate 360, Zoom
* **Deliverable**: Mandatory security and awareness training completed by all employees, including phishing simulations

**Full Rollout of MFA and Least Privilege (Duration: 2 Months):**

* **Start Date**: July 1st, 2025 (Month 7)
* **End Date**: August 31st, 2025 (Month 8)
* **Resources**: IT Security Team, Microsoft Azure
* **Deliverable**: MFA and least privilege implemented across all systems within the organization, with compliance achieved and confirmed through internal audits and user feedback

**Continuous Monitoring and Final Review (Duration: 1 Month):**

* **Start Date**: September 1st, 2025 (Month 9)
* **End Date**: September 30th, 2025 (Month 9)
* **Resources**: IT Security Team, SolarWinds
* **Deliverable**: Final audit report verifying compliance with PCI-DSS and GDPR, along with a continuous monitoring plan in place for ongoing security

H.  Project Evaluation

1.**Formative and Summative Test Plans:** Formative testing will occur throughout the deployment of MFA and least privilege controls, using ongoing vulnerability scans and system audits. Tools such as SolarWinds will be used to monitor access controls and detect issues early, while summative testing will be conducted after full implementation. This includes any final audits and penetration testing to ensure compliance and effectiveness of the new controls.

2.**Minimal Acceptance Criteria and Key Performance Indicators:** The minimal acceptance criteria will include the complete implementation of MFA across all critical systems and enforcement of least privilege through RBAC, as well as user training completion through our security awareness and training program. Key performance indicators will let us easily track any unauthorized access incidents, successful phishing simulation responses, and also will help achieve compliance with PCI-DSS and GDPR standards as outlined in the project goals.

**3. Test Cases and Scenarios**: Test cases will focus on scenarios such as unauthorized access attempts, phishing attack simulations, and user privilege audits. As for MFA, test scenarios will include verifying the multi-factor authentication process across various access points and for least privilege, test cases will ensure that users only have access to necessary systems based on their roles using Role-Based Access Controls.

**4. Analyzing Results:** Results will be analyzed through audit logs, penetration test reports, and user feedback from training sessions. Successful implementation will be measured against our Key performance Indicators, and any deviations achieved through feedback or other means, will be addressed with the needed adjustments to access controls or require users to undergo additional training. This will be found through our iterative approach using feedback, and we also will use continuous monitoring. Lastly, regular reporting will be used to ensure results are aligned with our compliance and security objectives set by executive management.

I.  References/Citations

PCI Security Standards Council. (2017, February). *Multi-factor authentication guidance v1.0*. Retrieved from <https://listings.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf>

**Reference list entry:** Cybersecurity and Infrastructure Security Agency. (n.d.). *Multifactor authentication (MFA)*. U.S. Department of Homeland Security. Retrieved from <https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication#:~:text=The%20use%20of%20MFA%20on,a%20user's%20identity%20for%20login>.

YouAttest. (n.d.). *The principle of least privilege for cybersecurity*. Retrieved from <https://youattest.com/blog/the-principle-of-least-privilege-for-cybersecurity/>

SolarWinds. (n.d.). Compare audit and full versions of Access Rights Manager. SolarWinds. <https://www.solarwinds.com/access-rights-manager/compare-audit-and-full-versions>

Microsoft. (n.d.). Microsoft Entra pricing. Microsoft. <https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing>

Articulate. (n.d.). Articulate 360 pricing options. Articulate. <https://access.articulate.com/support/article/Articulate-360-Pricing-Options>

Cofense. (n.d.). PhishMe security awareness training (SAT) platform. Cofense. <https://cofense.com/phishme-security-awareness-training-(sat)-platform>

Zoom. (n.d.). Plans & pricing. Zoom. <https://zoom.us/pricing>