Essay 1: In your disaster recovery plan, what is the most significant aspect of your plan and why? (particular risk, particular process, particular control…)

As cyber-attacks keep becoming more advanced, methods like phishing are still a major cause of data breaches, financial loss, and operational problems in organizations. The way that phishing attacks achieve this crippling result on organizations is by preying on its most vulnerable asset - the humans.

Among other forms of cyber-attacks, the likelihood of phishing attacks is more likely, due to the relatively easier method of execution, and the result is more significant too, due to its potential to leak data, slow down operations, and undermine trust. To fight against this simple, yet effective method of gaining sensitive information, we should train employees better, do in-house exercises (for example, sending fake phishing emails to employees to see who is more averse to revealing information), and incorporate better response protocols and security controls.

The significant aspects of my Disaster Recovery Plan:

1. **Employee Training and Awareness:**
    - This is the control I would implement first as it is the *fastest* and *most cost effective* way to immediately reduce our risks of falling for a phishing attack.
    - We would train employees regularly on the latest phishing tactics and give them real-world examples. This would make them better equipped to identify suspicious communication and respond correctly.
2. **In-House Phishing Simulations:**

    Conducting simulated phishing attacks will help identify employees who may be more susceptible to phishing attacks. This would enable us to tailor any further training to those individuals and improve overall resilience.

3. **Incident Response Protocols:**

    Having a well defined incident response plan will allow for quick action in the event of a successful phishing attack. This would include immediate reporting, isolating affected systems, and doing post-incident analysis to prevent any future occurrences.

4. **Enhanced Security Controls:**

    Using technical measures like filtering emails and two-factor authentication, will provide additional layers of protection against phishing attacks, thus reducing the risk of data breaches.

5. **Continuous Improvement:**

    Regular assessments/audits and updates to our disaster recovery plan will ensure it remains effective against evolving threats, including phishing. This

would include reviewing and testing the success of training programs and the effectiveness of our incident response measures.

As phishing attacks continue to pose a threat to organizations all over the world, it is important to realize the severe impact they can have and have proper measures in place to avoid or reduce its impact. . By focusing on employee training and increasing awareness, organizations can enable their staff to recognize and respond to phishing attempts effectively. Conducting in-house phishing simulations will allow us to better prepare, by identifying individuals who may need more support. Having a great incident response plan is also crucial, as it would allow us to quickly and effectively react to a phishing attack. Furthermore, enhanced security controls, such as email filtering and two-factor authentication would serve as first line defences against any attempts at an attack. In conclusion, by adopting these methods in our organization, we would better prepare ourselves against attacks, safeguard our assets and data, and keep operating without any problems to our customers or employees.

Essay 2: You are pitching to your CEO what controls your company must implement first. What controls will you propose in terms of cost, speed of implementation, impact of overall security.

While pitching controls to enhance our company's cybersecurity posture, I would propose an approach that would prioritize cost-effectiveness, speed of implementation, and significant impact on overall security.

1. Employee Awareness Training

Cost: Low to moderate, depending on the training platform or materials we might use.
Speed of Implementation: Fast - training sessions can be organized within a few weeks.
Impact: High - well-trained employees are the first line of defense against cyber attacks. By educating employees on recognizing phishing attacks, social engineering tactics, and safe online behaviors, we can significantly reduce the likelihood of successful attacks.

2. Multi-Factor Authentication

Cost: Medium - may involve subscription costs for some MFA services but we could also implement it using existing tools and code.
Speed of Implementation: Fast - MFA can usually be deployed within weeks or for most applications.
Impact: High - MFA adds an essential layer to our security, making unauthorized access much more difficult even if passwords are leaked. This control would be particularly effective for accessing sensitive systems or data.

3. Email Filtering

Cost: Medium - initial setup costs for filtering solutions may be low but also offset by subscription fees in the future.
Speed of Implementation: Fast - deployment can be completed in a matter of weeks.
Impact: High - by implementing robust email filtering, we can significantly reduce the volume of phishing emails that reach employees, thereby lowering the risk of successful attacks.

4. Regular Software Updates and Patches

Cost: Low to Moderate - This would primarily involve labor costs for IT staff to manage updates.
Speed of Implementation: Making updates is an ongoing process, and the speed of implementation would usually depend on the update or patch being made.
Impact: High - Keeping our software up to date would minimizes the number of vulnerabilities that attackers can exploit, thus reducing our overall attack surface.

5. Developing an Incident Response Plan

Cost: Low to moderate - This would mainly involve the time of staff to develop and document the plan.
Speed of Implementation: Moderate - Drafting and formalizing the plan may take several weeks to be completed.
Impact: High - Having a well-defined incident response plan, once completed, would allow us to react quickly and efficiently to security incidents, thus minimizing damage and recovery time.

6. Network Segmentation

Cost: Moderate - This would involve configuration changes and possible investment in a bit of hardware.
Speed of Implementation: Slow; may take weeks to months depending on the complexity of our network.
Impact: High - Networks, once segmented, would limit the movement of attackers within the organization and protect sensitive data and critical systems from being accessed by any threat actors.

Implementing these controls would provide a strong foundation for our cybersecurity posture while balancing cost, speed, and impact. By prioritizing employee training, multi-factor authentication, and email filtering, we can

address our most important vulnerabilities quickly and effectively, while making sure that our organization remains well protected against evolving threats.