Student:	Email:
Bradley Adams	badams10@my.athens.edu

Time on Task:	Progress:
	100%

Report Generated: Tuesday, February 18, 2025 at 12:33 PM

Guided Exercises

Part 1: Research Organizational Structures

5. **Discuss** how employee behavior changes depending on the organizational structure in which the employee works.

With over 30 years of work experience, I have worked in flat, hybrid, and hierarchical structures. I've also spent the last 20 years experiencing significant growth in my current position, observing the transition from a hybrid, flat-leaning to a solid hierarchical structure. I have co-owned a successful small business start-up with five people, worked for a few medium-sized DoD contractors, and worked for the fastest-growing and largest city in Alabama, which employs approximately 2,130 full-time and 320 part-time employees. Based on the resources in this lab and my personal experience, the following are some employee behavior changes that occur depending on the organizational structure.

Multiple layers of management depict hierarchical structures. Authority flows from top executives to frontline employees, with each level overseeing the one below it. This design can result in well-defined roles and responsibilities. Decisions are created at the upper management levels. Employees are expected to obey set policies and procedures. This leads to a culture of conformity to formal methods. This approach can provide consistency and control but may suppress creativity and limit honest communication. Focusing on top-down communication can make employees less creative. Upper management usually sets policies and communicates those policies down a chain of command. The top-down approach creates uniformity and control but may restrict employee input.

Flat organizations have minimal hierarchical levels, fostering a more even or equitable workplace. This structure promotes open communication and collaboration across operations. Employees often have more freedom and involvement in decision-making. The reduced emphasis on management direction can create a culture of innovation and flexibility. Employees can take initiative and contribute to the organization beyond their primary roles. This sense of empowerment can improve job satisfaction and a sense of ownership. Flat structures can cause employees to feel uncertain about their responsibilities and expectations. This freedom can pose challenges in policy enforcement, as monitoring actions and administering disciplinary actions can become less formal. Policy development can involve employees at different levels, which can improve employee buy-in.

Part 2: Create a Policy Framework Implementation Plan

Publish Your Policies for the New Clinic
Explain your strategy

Specialty Medical Clinic: Policy Framework Implementation Plan

United Medical Services (UMS) is acquiring Specialty Medical Clinic (SMC). It is necessary to integrate UMS's hierarchical security policy framework into SMC's existing flat structure. This implementation plan will provide compliance with IT security standards and adapt the differences between UMS and SMC.

The strategy will involve a structured, phased approach to merge policies without disrupting operations.

Phase 1
Conduct a thorough review of the SMC's security policies and compare them with UMS's hierarchical framework. Engage with executive leadership, IT security personnel, Human Resources, and staff to understand concerns and promote buy-in. Tailor the security policy framework to bridge the two structures and preserve the elements valued in SMC's culture.

Phase 2
Draft updated security policies that align with UMS's existing framework and provide clarity for SMC's employees. Implement a structured communication plan with emails and documentation to educate employees on policy change. Conduct security awareness training covering policy compliance.

Phase 3
Modify system permissions, network access, and authentication criteria to conform to UMS policies. Implement system logging, content, and email filtering to secure policy adherence. Implement a monitored system for reporting security violations to IT security personnel.

Phase 4
Align disciplinary actions for policy violations with UMSs. Ensure staff, contractors, and consultants know new security policies. Conduct routine compliance reviews to assess compliance with the new framework.

Phase 5
Perform a tri-annual security audit for the first year to assess the integration's effectiveness. After the first year, perform bi-annual security audits. Establish an open feedback process for employees to provide input on policy implementation and potential improvements. Adjust policies to align with evolving security threats and organizational needs.

Implementing this strategy will make the transition efficient. This strategy will provide security compliance and minimal disruption to clinic operations. This strategy fosters an organizational culture of security awareness while preserving the strengths of SMC's existing structure.

Communicate Your Policies to the New Clinic Employees

How are you going communicate policies to employees?

Draft updated security policies that align with UMS's existing framework and provide clarity for SMC's employees. Implement a structured communication plan with emails and documentation to educate employees on policy change. Conduct security awareness training covering policy compliance.

Involve Human Resources and Executive Management

How would you smoothly involve HR and executive management?

I would engage with executive management early. I would schedule meetings with UMS leadership to review the importance of policy integration and secure their commitment. I would outline how the hierarchical security policies will be adapted while respecting the existing SMC culture. I would encourage the CEO and executive team to endorse the policies actively. I would show a clear structure where executives oversee policy enforcement, providing alignment with UMS’s strategic objectives.

As for Human Resources, I would work closely with HR to revise employee handbooks and training materials. Encourage HR to host training sessions to educate employees on policy expectations, disciplinary procedures, and compliance requirements. I would work with HR to implement a feedback process where HR can get employee input.

Incorporate Security Awareness and Training for the New Clinic

How do you make the training fun and engaging?

I would incorporate interactive quizzes with rewards, use real-life simulations and case studies that employees respond to, use storytelling and humor with videos, use scenarios and challenge employees to identify policy violations and provide incentives for participation such as gift cards or extra breaks. I would also acknowledge employees who consistently applied security practices in actual work. A fun and engaging experience is a 'cybersecurity escape room' in an in-person or virtual escape room. Employees must follow security policies and best practices to 'escape' the simulated security breach.

Release a Monthly Organization-Wide Newsletter

How can you make this newsletter succinct and informative?

Create bullet points and subheadings that help staff quickly scan for key takeaways. Make each section concise and relevant to employee responsibilities. Include clear instructions and action items. Highlight important details with visuals such as emojis or icons. Recognize employees for security awareness and include interactive elements like training events. Keep the newsletter engaging, easy to read, and informative, and ensure compliance stays a priority.

Implement Security Reminders on System Log-in Screens

Which critical systems would you deploy these to?

After researching critical systems for a medical specialty organization, I would deploy login screen security reminders to several critical systems, including any electronic health records (EHR) system that accesses patient data and any Hospital Management System (HMS), which will ensure secure access for scheduling, billing, and administrative functions. I would also remind users of safe access procedures for Remote Access, such as VPNs. Apply login screen reminders on workstations that interact with HIPAA data. I would have login screens on any Medical Imaging and Diagnostic system.

Incorporate Ongoing Security Policy Maintenance for All

How will you review and obtain feedback from employees and policy-compliance monitoring?

I would implement a structured ongoing security policy maintenance plan. The plan would focus on regular policy reviews, employee feedback collection, and compliance monitoring. Quarterly audits would identify gaps and provide updates. I would also adjust policies to comply with HIPAA and other applicable local, state, and federal laws and regulations. I would distribute surveys bi-annually and collect training feedback forms after training to review employee feedback. I would review system logs, access control monitoring, and anomaly detection systems to track policy compliance. I would have IT security personnel conduct random audits on employee workstations and login activity. I would develop a monthly newsletter program to share updates, best practices, and compliance topics. Leadership briefings quarterly would update executive management on compliance and any policy change recommendations.

Obtain Employee Questions or Feedback for Policy Board

How will you review and incorporate employee questions and feedback into policy edits and changes as needed?

I would create a continuous improvement plan that involves employee feedback in the policy review process. This plan would allow employees to contribute insights and knowledge to policy development. Employees can ask questions and give suggestions for improvements. I would have an email address such as policyfeedback@specialtymedical.com for employees to submit questions or voice concerns. IT personnel could secure an anonymous submission form online for employees to provide anonymous feedback. Open meetings quarterly allow employees to discuss problems directly with the policy board. Each department could appoint a representative to collect concerns and feedback, and that representative could present the input to the policy board.

The policy board could categorize feedback into priorities such as urgent, which would be reviewed within 24 hours, or immediate, which would be reviewed within ten days. The policy board would review any general suggestions quarterly during review meetings.

I would share quarterly feedback and policy adjustment overview reports with employees, reinforcing employee influence on policy development. I would acknowledge contributors who supplied valuable input leading to policy improvements.

This plan would ensure policies stay practical, effective, and aligned with employee requirements. This approach encourages a culture of security awareness, transparency, and continuous policy improvement.

Challenge Exercise

Compile a list of videos that would provide a total of 30 to 45 minutes of content, organizing the videos in an order that you believe would best supply the appropriate security awareness training.

1. Social Media Video Lesson - 7:23 Minutes
https://www.youtube.com/watch?v=bGSjUYLTODE
While there are many benefits to sharing and communicating through social media, it can also be a big security risk. This video lesson explores the risks associated with social media and why you should be concerned.

2. Social Media Mining by Insider Threats - 1:44 Minutes
https://www.youtube.com/watch?v=ydT8I-2yIW8
Social media users often trust companies like Facebook and Twitter to protect their personal information. Users might not consider the risk of bad actors within these companies and how an insider's motivations might lead to a malicious act, such as espionage.

3. Social Engineering: Why It Matters - 13:33 Minutes
https://www.youtube.com/watch?v=lEwC1tN2jb8
Social engineering is one of the largest threats to an organization as the attack is targeted and can come from a variety of avenues. Social Engineering uses manipulation, influence, or deception on the victim to gain access to personal or financial information, as well as control over a computer system or network. Social engineering uses the exploitation of a trusted relationship with trusted access by using deception and manipulation to convince the victim to click on a malicious link or attachment, give information, or reveal credentials.

4. Ransomware - 10:23 Minutes
https://www.youtube.com/watch?v=txhV55Vr1gA
Ransomware attacks are on the rise. Ransomware "kidnaps" your data and demands ransom. This video lesson guides you through an attack and discusses what you need to know to protect yourself.

Total of 32:23 minutes

Explain your security awareness training program and its purpose.

This security awareness training program familiarizes employees with the risks associated with social media, social engineering, and ransomware. By understanding these cybersecurity threats, employees can protect the organization from cyberattacks. This program provides fundamental lessons from four security awareness videos for 32:23 minutes of training. It's structured to be simple, engaging, and practical.

This program will cover key risks associated with social media, such as oversharing personal information, cybercriminals using publicly available information for attacks, risks of fake accounts and impersonation, and data privacy concerns. The program covers social media mining to understand the misuse of access to data and the motivations. The program will cover social engineering attacks such as phishing, pretexting, baiting, and tailgating. Lastly, the program covers ransomware awareness, explaining to employees how ransomware works and best practices to prevent an attack.

This program aims to familiarize employees with staying alert against these threats, applying best practices in cybersecurity in their day-to-day work, and reporting any suspicious activity to the IT security team.