QUESTION #2:   
(addressing SLO #2 - summarize and explain organizational development and strategies common to technology-intensive enterprises & SLO #3 - formulate and assemble component ideas in order to successfully execute a project plan)

NOTICE: The following questions are to be answered in your own words. Your responses to the questions are to be formulated solely from your personal body of knowledge developed and derived from your readings, study and research while in the Master of Science in Technology Management degree program. Quotations, citations or other materials included in your question responses must not come directly from the writings or research of others. Your responses are to be detailed and specific.

The Information economy is one of the most important values of society that is heavily dependent on cyber security. On an international and national scale cyber-attacks are occurring more frequently and becoming increasingly more complex. It is evident that the development and deployment of an international security strategy is critical in an interconnected world.

**Questions to be answered:**

1. Describe how organizational structure, culture and decision making strategies play a key role in the effective implementation of cyber-security.
2. What ethical implications must be considered and addressed by the technology manager in implementing these strategies?

C:\Program Files\Microsoft Office\MEDIA\OFFICE14\Lines\BD14801_.gif

**Question (A):**

**Organizational Development and Strategies Common to Technology-intensive Enterprises:**

**The implementation of cyber-security**

The topic of cyber-security is of major interest on a national and international scale. From my understanding, the threats of cyber-security include formidable criminals systematically infiltrating intellectual property and, according to Moeller (2011), even the most dangerous and threatening adversaries are acquiring tools and efforts of disrupting critical services, which supports the world information economy, public safety, and general security. For instance, I consider one of the strategies at the fore is information sharing, which is an important element of a policy for effective cyber-security. In a national and international scale, it is necessary and important to create and establish changes in attitudes towards changing the organizational culture (Trim and Upton, 2013). In this case, cultural change, based on my view, refers to the immediate realization and understanding that IT security is important considering failure in security is potentially adverse across the board.

In technology-intensive enterprises, organizational structure and culture are partly characterized by the use of cyber capabilities for various information operations, reconnaissance, for cyber-attacks, and disruption of important networks and services as well as information operations and electronic warfare, according to Moeller (2011). I affirm that one of the organizational structure, culture, and decision-making strategies, both nationally and internationally, include the recognition of the power and impact of corporate culture to redesign the attitudes and behaviors of employees. This way, many cyber-security and IT leaders are in the process of instilling a culture of cyber security in their organizations. It is important that employees' everyday actions and decisions are imbued with extreme cyber-security awareness. I view this, drawing from my readings, as an important strategy to improve organizational ability to prevent cyber-attacks, safeguard data, protect shareholders' value, and reduce the level of risks.

Secondly, the organizational culture strategy I would also consider changes in behavior, which includes creating awareness on matters of security amongst senior executives, which according to Trim and Upton (2013), should not be entirely reactive. Based on my understanding of this strategy, taking a more proactive approach or stance would help in effectively tackling most of the emerging challenges and compliance issues. Security awareness is the first move, which should begin with changing behavior. For instance, one example I would give is that the management (as opposed to the corporate), as part of the decision-making strategy, should take personal responsibility for matters security. I see this as one of the decision-making strategies to create awareness within the organizational setting and, therefore, this will create a different awareness level into the organizational culture.

Thirdly, organizational structure strategies are important in protecting data and intellectual property. I have always known that the most notable challenges include difficulty in safeguarding an organization's data as well as the intellectual property, which according to a study by Trim and Upton (2013) refers to the information that largely comprises the quantity of an institution's value. Given the emergence of collaborative cultures and new technologies, which include the use of mobile devices makes it extremely difficult to protect information and intellectual data. Moeller (2011) noted that cyber security goes beyond the protection of intellectual property to processing its application that includes strengthening, securing, and making it more reliable. Therefore, of the strategies that I know could aid in the implementation of cyber-security is the strong identity management that helps in controlling those gaining access to data and information and with what kind of permissions.

Finally, there is a shift from technology to security management, a strategy that I consider to be as important in an effective implementation of cyber security. Security once focused more on providing organizations with solutions; today, this strategy focuses on providing governance, consultancy, and policy development in tackling cyber-security. Part of the organizational culture comprises the senior management taking part in joint ventures and outsourcing as well as developing a security culture towards setting the right tone and direction at the top level. Additionally, this strategy will allow senior level executives to take part in and support any cyber-security policies and strategies.

**Question (B): Ethical Implications:**

While implementing these strategies, the technology managers must consider and address ethical implications, which involves breaching of networks, compromised personal identification data, stealing of personal identities, personal financial ruin, and classified government secrets (Brennan and Johnson, 2004). The technology managers must focus more on employee personal data that may be critical in employees' confidentiality, which in my opinion, is an important move towards avoiding compromise on personal identities. Technology managers' failure to secure the organizational systems is due to their failure to consider those employees using information that should not have been accessed in the first place as well as those finding shortcuts and breaches around well-developed security procedures.

Technology managers should establish ways of monitoring everything that employees do and how technology operates. In my view, one of the major ethical implications to be considered is individual privacy. While tackling issues related to cyber security and cyber-attacks, it is unethical for organizations to access or track employee personal information without their consent, employee movements or even potential customers. While formulating strategies to protect the organization from cyber-attacks, I think it is important for technology managers to put into considering privacy issues, which includes collecting personal data. Again, this can also be done by recognizing that those involved in cyber-attacks are young people who may need assistance in tapping their skills and using it as part of cyber security without these technology managers handling the issue unethically by exposing them and their information to the public and, thus, makes it easy for them in handling the issue.

Technology managers should also consider issues related to security in the organization. According to Lenk et al. (2007), organizations monitor visitors and employees and gather additional personal information in the name of handling security matters. In this case, a number of ethical issues arise, especially when it involves continuous monitoring and recording of employees' activities and images, an act I consider to be unethical since it involves breaching of employees' privacy in the name of security. The technology managers should understand that an unjustified act of managing employees is, in my view, questionable and unethical and should be considered before being addressed. It is important that these managers establish ways of monitoring and focusing on cyber-security, which is justifiable. For instance, I think that the non-employees' surveillance in an organization must be constrained in an ethical level.

Finally, technology managers must consider and address ethical implications that touch on content. I understand that with the continuous emergence of new technologies, it allows for easy development and distribution of videos and images and, thus, it is important that these managers must require acceptable guidelines to consider and address. A lack of these guidelines could be offensive to staff members as well as the public. It is important for technology members to come up with these guidelines accompanied by the restrictiveness in considering acceptability in tackling any emerging ethical issues that touch on individual lives and the organization's security. Additionally, I understand the issue of communication is pertinent and, thus, it is important for technology managers to put measures in place to scan those text messages and phone calls that only detrimental to the security of the institution. It is important that any ethical implication touching on surveillance be considered first.

**References**

Brennan, L. L., & Johnson, V. (2004). *Social, ethical and policy implications of information technology*. Hershey, PA: Information Science Pub.

Lenk, C., Hoppe, N., &Andorno, R. (2007). *Ethics and law of intellectual property: Current problems in politics, science, and technology*. Aldershot, Hampshire, England: Ashgate.

Moeller, R. R. (2011). *Cyber security and privacy control*. Hoboken: John Wiley & Sons, Inc.

Trim, P. R. J., & Upton, D. (2013). *Cyber security culture: Counteracting cyber threats through organizational learning and training*. Farnham: Gower.