**Case-2: PharmaCo by Blake DeLong and Rithu Anand Krishnan**

Q1 - As CISO, this is my assessment of PharmaCo’s governance and control of cybersecurity risks.

**Identify**: Analyzing the case and their SEC filing, it is evident PharmaCo has a well-developed system of identifying data assets and their associated cyber risks. Despite his recent appointment, PharamCo’s new CISO, Paul Williams, has inherited an IT system that recognizes the risk surrounding both confidential employee information and sensitive HIPPA data. Understanding the risk, Williams has created businesses continuity, response, and recover plans in the eventuality that a breach occurs. Additionally, the company’s SEC filings points out that the shift to work-from-home introduces new cyber risks that are being addressed, demonstrating a forwarding thinking mindset of the company leadership.

**Protect**: Likewise, the ‘Protect’ component of the NIST framework is also fairly mature. PharmaCo has taken a defensive data strategy posture by separating and encrypting data assets that the company holds while also ensuring their security with multiple off-site encrypted backups. When combined with the data policies created by Williams, this combination of physical security infrastructure and logistical security planning bodes well for a company who has not yet had to learn from a costly mistake.

**Detect**: As mentioned, PharmaCo’s data security infrastructure and planning has been tested by neither professional Penetration Testing nor an actual malicious attacker. Because of this, the ‘Detect’ component of the framework is not as mature. Instead, we would rather like to see that the IT security team is continuously testing their own detection methods to ensure that the infrastructure and procedures they have in place are performing to expectations or identifying any weaknesses. In their own admittance, PharmaCo only rates their maturity as ‘Initial’ due to its current informality.

**Respond**: Likewise, the ‘Respond’ component is also very immature in its implementation because it is untested. Testing response to malicious activity commands simulations where policies are put into action and practiced. To PharmaCo’s credit, testing is planned for Q3 of the financial year, but this component must be considered immature until cyber breach response is tested to identify inevitable issues.

**Recover**: Finally, the ‘Recover’ component is also fairly immature. While PharmaCo has the data asset backup infrastructure to recover from a data loss event, the policies, again, need to be tested to validate their practically effectiveness.

In conclusion, I recommend that we negotiate terms that ensure PharmaCo will first engage with a third-part IT security to thoroughly test their detection, response, and recovery capabilities before the companies can merge. In addition to my analysis above, I recommend PharmaCo undergo this testing because they already plan to in Q3 and Q4 of this year, per the case. It would be fiscally wise to let them incur that cost themselves.

Q2 - A company should treat cybersecurity as an enterprise-wide risk because a cyberattack can disrupt critical infrastructure, causing an enterprise-wide impact. As the CISO of PharmaCo, you have implemented sophisticated policies and procedures for data protection. It is critical to have IT professionals focusing on security and cybersecurity with specific responsibilities. Still, the CISOs should also comprise the CEO, board, and department managers, along with key vendors, partners, and stakeholders. Having each of those stakeholders and directors informed about their cybersecurity roles will help ensure that the company has a robust risk management strategy. PharmaCo has about 12 directors with a good mix of industry experience. I would ask you what steps were taken in training the directors about cybersecurity. Does PharmaCo have certified cyber risk training sessions that are mandatory for the directors and, if so, is this training updated regularly according to new policies?