**Class Activity**

**Name: Saman Khan**

**ID: 19K-0354**

**Section: H**

It is difficult to envision a more problematic year for data security than 2020. The pandemic resulted in millions of employees working from home overnight. More serious cyber threats, including those posed by highly sophisticated state actors, posed a threat to enterprise databases. Natural catastrophes also impacted regional enterprises and supply systems. In the second half of 2020, we interviewed 57 technology professionals, including chief information officers, chief information security officers, chief data officers, and other public- and private-sector business leaders, to determine how firms responded to this perfect storm of cyber threats. Cyber resilience, or the capacity to endure unplanned disruptions, is no longer just the responsibility of IT activities, according to the report. Rather, enterprises require a comprehensive approach to cyber resilience as data becomes more widespread across company operations and departments in order to improve business performance. Specifically, they require a comprehensive data management strategy and cross-functional data security responsibilities. The majority of organizations were unprepared for the epidemic and the ensuing shift to working from home. Businesses permitted company and function executives to make ad hoc, patchwork arrangements to meet the demands of their personnel. Consequently, IT and security teams were frequently unaware of the devices used by employees, the applications on those devices, whether they had the necessary security patches, the security of Wi-Fi connections, or the prevalence of other connected devices, such as gaming consoles and smart devices. Cyber risk increased exponentially as a result of the resultant free-for-all enforced for the sake of business continuity. Cyber-attacks quadrupled in 2020 compared to previous years, mostly owing to malicious actors abusing insecure virtual work environments and improvised IT infrastructures. 1 These attacks cost firms an average of hundreds of thousands of dollars, but frequently much more, and are a role in the demise of many small and medium-sized organizations. 2 Even though cyber-attacks are expected to cost U.S. businesses close to $1 trillion by the end of 2020, a survey of over 1,000 enterprises revealed that only 44 have cyber readiness and incident response plans in place. Worse, only 32 believed the plan was genuinely effective, and the board or executive suite was often not involved in its development. Even more frightening was the recent Solar Winds attack on government and Fortune 500 corporations. The breach exposed sensitive data to roughly 18,000 firms using Solar Winds IT management and network monitoring software for eight months. 4 Worse, the breach paved the way for other thieves. It could take months, if not years, to determine the full impact of the supply chain harm. There is no way back now. Data is a vital source of competitive advantage for firms across all industries, and the speed of digitization will only intensify. Simultaneously, the potential of disruptions and malicious assaults puts company data at an increasing risk. Given this complexity, firms require a comprehensive approach to cyber resilience that is anchored in data management and covers responsibilities throughout the organization. Data management is the process of gaining access to, storing, organizing, and preserving an organization's created and acquired data. Companies must guarantee that data is accessible, comprehensible, linked, trustworthy, and secured. 5 Moreover, data needs to be safe in transit from point A to point B across a computer network or IT environment because network interfaces are often the major sites of vulnerability to outsiders. Addressing data management involves answers to several crucial questions Where does the data come from, and where does the data reside in the organization for example, in databases, data warehouses, or data lakes How often does data change, and how is it distributed around the company over time? Who has access to data, such as IT personnel or internet-of-things devices or processes from another network? How is data utilized For instance, is it converted or fed in raw form to the company's crucial systems? How can data be quickly accessible or secured during a crisis such as a natural disaster? How is the data reviewed in the event of a cyber-attack to ascertain if it has been compromised? How does the company track the movement of infected data throughout its IT architecture? In addressing each of these challenges, businesses must strike a balance between making data accessible so that business units and functions may utilize it to produce value and guaranteeing its security. In addition, they must comprehend the landscape of potential threats and plan for their detection, reaction, and recovery. Due to the magnitude of both the planning and execution of this endeavor, the entire company must be involved. IT and security professionals need actionable data on everything in the network, not just the devices and applications that employees use daily, for cyber resilience to function. This involves up-front planning to model scenarios that will indicate how data is to be accessible, together with all conceivable touch points to the organizations network such as supply chain nodes. This level of situational awareness is significant and necessitates a cross-functional approach across critical positions. Chief data executive The CDO is accountable for all executive-level data management decisions, both during normal operations and in the event of a data breach. Creating and maintaining data classifications and categorizations for business-critical processes and associated systems is a fundamental responsibility of the CDO. The data categorizations come up to the CDO from data stewards within each business unit and function, each of whom has direct knowledge of his or her departmental data requirements. They are aware of which employees need access to particular data in order to do their duties, which systems or feeds should have access, and how operational performance might be affected if certain data were unavailable or tainted. Data stewards also check the accuracy of the data, promote exchanges with other entities, and chart the flow of data. Data is guarded by the IT team, which includes cyber security engineers and enterprise architects. They specify the routes via which data centers and exits company systems, as well as the access security protocols. Notably, the IT team also educates employees on data management, including work-from-home regulations, device restrictions, rules controlling company-owned devices, and network access. Human capital. The HR department maintains information on security clearances and work schedules, work-from-home policies, and employee needs such as virtual private networks. This information allows the cyber resilience teams to quickly spot abnormalities in employee’s access to essential data and more important to priorities access for certain individuals and work processes in the wake of an attack. The legal function, which includes personnel working on acquisitions and partnerships, coordinates with the CDO to ensure that vendors have contracts in place that specify reasonable reaction timelines in the case of a crisis.