Organizations' ever increasing technology reach has led to a surge in cybersecurity risks. The constant and ongoing threats of a cyber-attack require companies to continuously update defenses to prevent attacks as well as limit damages form a successful attack. We develop a dynamic differential cybersecurity game model between an attacker and defender (firm). The attacker can have multiple methods of attack each with separate probabilities of success and resultant payoffs. The firm meanwhile impacts the probability of successful attack by allocating resources to both prevention and containment strategies that reduce the probability of a successful attack or the resultant losses (attacker payoffs) respectively. We further consider the role of a third player, for example government agencies, that can use its resources to detect threats and provide information to a firm to increase the successful defense/containment strategies. We then solve for the equilibrium strategies, offering insights into effective cybersecurity approaches.