Incident handler's journal: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Scenario 1

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.

Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

Date: Record the date of the journal entry.	**Entry: 2023-10-05** Record the journal entry number. 001
Description	Provide a brief description about the journal entry.:Ransomware Attack on U.S. Health Care Clinic
Tool(s) used	List any cybersecurity tools that were used: SIEM (Security Information and Event Management)
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident?An organized group of unethical hackers known to target healthcare and transportation industries. ● **What** happened?The attackers used targeted phishing emails to gain access to the clinic's network, deployed ransomware, and encrypted critical files. A ransom note was displayed demanding payment for the decryption key. ● **When** did the incident occur?The incident took place on Tuesday morning, at approximately 9:00 a.m. (2023-10-03) ● **Where** did the incident happen?The incident occurred at a small U.S. health care clinic specializing in primary-care services. ● **Why** did the incident happen?The motive was financial gain through a ransom demand, and the attackers gained initial access through phishing emails.
Additional notes	Incident response was initiated immediately upon detection. Affected systems were isolated to prevent further spread. Law enforcement agencies and cybersecurity experts were contacted for assistance.

	Patient data is currently inaccessible, causing significant disruption to clinic operations. The clinic must decide whether to pay the ransom or attempt file recovery from backups. Steps are being taken to enhance email security and user training to prevent future phishing attacks.

In the scenario, a criminal group known as Scattered Spider initiated a cyber attack on MGM Resorts International, a global hospitality and entertainment company. The attackers used a social engineering attack to gain unauthorized access to MGM's network. They exploited human factors, including password reuse, and manipulated multi-factor authentication (MFA) to establish a foothold within the organization. Subsequently, the attackers escalated their privileges and compromised both Okta and Microsoft Azure environments. The incident led to the deployment of BlackCat/ALPHV ransomware on MGM's ESXi servers, impacting thousands of systems critical to the hospitality industry. This resulted in widespread disruptions, including the malfunction of hotel room keys, dinner reservation systems, point-of-sale systems, and slot machines. MGM Resorts estimated daily losses of up to $8.4 million in revenue.The incident highlights the significance of securing Identity and Access Management (IAM) platforms, the risks associated with social engineering attacks, and the importance of robust multi-factor authentication controls. It also underscores the need for swift incident response and ongoing efforts to recover from a cyber attack of this scale.

Date: Record the date of the journal entry.	**Entry:09/07/2023** Record the journal entry number.002
Description	MGM Resorts International Cybersecurity Incident - Response and Mitigation

Tool(s) used	Incident response tools, privileged access management (PAM) solutions, security information and event management (SIEM) systems, identity provider (IdP) best practices.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident?Scattered Spider, a criminal gang of U.S. and U.K.-based individuals. ● **What** happened?The attackers gained unauthorized access to MGM Resorts' network, escalating privileges and deploying ransomware that encrypted critical systems. In response, MGM Resorts initiated containment and mitigation measures. ● **When** did the incident occur?The incident began in the summer of 2023 and was discovered recently. ● **Where** did the incident happen?The incident occurred within MGM Resorts International's network, impacting their global operations. ● **Why** did the incident happen?The incident resulted from the attackers' social engineering attack, successful manipulation of multi-factor authentication (MFA), and exploitation of vulnerabilities in the IAM platform and IdP configuration.
Additional notes	Containment and mitigation efforts were initiated by MGM Resorts' incident response team, including the termination of Okta sync servers and credential harvesting techniques deployed by the attackers. The compromise of Okta and Azure environments was identified and addressed, but the damage had already been done. Subsequently, the BlackCat/ALPHV ransomware group was involved, encrypting ESXi servers and causing widespread disruptions to MGM Resorts' operations. The incident highlights the critical need for securing privileged accounts and

	implementing strong authentication measures, such as MFA controls. Recommendations include focusing on minimizing exposure of privileged accounts, implementing strong authentication measures, protecting Tier 0 assets, and monitoring trust changes to enhance security. MGM Resorts and other organizations must continuously improve their security measures to protect against evolving cyber threats and minimize financial and reputational damage. This incident response and mitigation entry emphasize the importance of swift action and the ongoing effort required to recover from a cyber attack of this magnitude.

Scenario: In September 2023, Indian hacktivists launched Distributed Denial of Service (DDoS) attacks on Canada's military and Parliament websites. These attacks significantly slowed down system operations for several hours. The hacktivists were motivated by Canadian Prime Minister Justin Trudeau's public accusation against India in connection with the killing of Sikh independence activist Hardeep Singh Nijjar. This incident underscores the impact of politically motivated cyber attacks and the importance of robust cybersecurity measures for government and military entities.

Date: Record the date of the journal entry.	**Entry:09/21/23** Record the journal entry number.003
Description	DDoS Attacks on Canadian Military and Parliament Websites
Tool(s) used	DDoS mitigation tools, incident response tools.
The 5 W's	Capture the 5 W's of an incident.

	● **Who** caused the incident?Indian hacktivists targeting Canada's military and Parliament websites. ● **What** happened?The hacktivists launched Distributed Denial of Service (DDoS) attacks on Canada's military and Parliament websites, causing system operations to slow down significantly for several hours. The motivation for the attack was the public accusation made by Canadian Prime Minister Justin Trudeau against India regarding the killing of Sikh independence activist Hardeep Singh Nijjar. ● **When** did the incident occur?The incident occurred in September 2023. ● **Where** did the incident happen?The incident targeted Canada's military and Parliament websites. ● **Why** did the incident happen?The incident was a retaliatory action by Indian hacktivists in response to the accusations made by Canadian Prime Minister Justin Trudeau against India
Additional notes	The DDoS attacks caused a disruption in the operation of Canada's military and Parliament websites for several hours. The attack was politically motivated and aimed to protest the accusations made by the Canadian Prime Minister regarding the killing of the Sikh independence activist. DDoS mitigation tools were employed to manage and mitigate the impact of the attacks. It is essential for organizations, especially government and military entities, to have robust DDoS mitigation strategies and incident response plans to address such incidents promptly. This entry highlights the DDoS attacks on Canadian military and Parliament websites, emphasizing the significance of cyber attacks with political motivations and the need for strong cybersecurity measures to protect critical

	government infrastructure.