SCENARIO #1: **Eternal Blue Ransomware Attack**

Scenario:

On May 7, 2019, the city of Baltimore, Maryland, experienced a ransomware attack that significantly impacted its online services. The attackers seized control of the majority of the city's servers and issued a ransom demand of 13 bitcoins for their release [1,2]. The global WannaCry ransomware utilized the cyberattack exploit EternalBlue, originally developed by the National Security Agency (NSA). Although a vulnerability in the Windows OS had been discovered earlier, the NSA opted not to report it to Microsoft. Instead, they developed a cyberattack exploit based on this vulnerability, as testified by former NSA employees [3,4]. Despite Microsoft releasing patches in March 2017, a substantial number of unpatched computers globally allowed the cyberattack to persist until recently.

WannaCry exploits a vulnerability in Windows SMBv1 (Server Message Block), enabling "remote code execution" [5]. Upon infecting a vulnerable Windows system, the ransomware encrypts files and demands payment for decryption. Specifically, SMB is a network communication protocol facilitating shared access to files and printers among computers on a network. However, Microsoft's implementation of the protocol harbors several security vulnerabilities, permitting the execution of arbitrary code on the target computer. This vulnerability is susceptible to well-known buffer overflow attacks.

In the context of the OCR Virtual Machine, students will practically implement this scenario, utilizing Linux (attacker) and Windows (victim). They will delve into the details of the WannaCry attacks and explore countermeasures. Additionally, students will discuss strategies to alert and address vulnerabilities on unpatched machines globally. The course will cover the legal and business risks associated with ransomware, examining the legal and strategic considerations when responding to a ransomware attack.

Key topics include: (1) Identifying and applying relevant state, federal, and international data breach reporting laws. (2) Analyzing the technical information required to trigger a legal reporting requirement under different laws. (3) Examining the legal and strategic issues related to deciding whether to report a breach to law enforcement. (4) Exploring the potential application of state, federal, and international/foreign data privacy laws. Students will compare this case with other similar recent incidents in Atlanta, Georgia, West Haven, Connecticut, Valdez, Alaska, and Roseburg, Oregon, along with their respective responses. Given the ongoing prevalence of unpatched computers and persistent cyber threats, students will discuss strategies to enhance cybersecurity awareness, particularly within public offices.

NICE Workforce Framework for Cybersecurity:

Scenario #1 & #2 will cover the following Knowledge areas.
K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0004 Knowledge of cybersecurity and privacy principles.
K0005 Knowledge of cyber threats and vulnerabilities.
K0049 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
K0116 Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
K0131 Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.
K0205 Knowledge of basic system, network, and OS hardening techniques.
K0210 Knowledge of data backup and restoration concepts.
K0373 Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
K0392 Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
K0452 Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.
K0627 Knowledge of the importance of ingress filtering to protect against automated threats that rely on spoofed network addresses.

References:

[1] A Timeline of the Baltimore City Ransomware Attack, https://cyware.com/blog/a-timeline-of-the-baltimore-city-ransomware-attack-d006
[2] Baltimore, $18 Million Later: 'This Is Why We Didn't Pay the Ransom', https://www.secureworldexpo.com/industry-news/baltimore-ransomware-attack-2019
[3] Nakashima, Ellen; Timberg, Craig (May 16, 2017). https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html
[4] Greenberg, Andy (May 7, 2019). “The Strange Journey of an NSA Zero-Day-Into Multiple Enemies' Hands". Wired. Archived from the original on May 12, 2019. https://www.wired.com/story/nsa-zero-day-symantec-buckeye-china/
[5] HIRT-PUB17008 : Security Alert: Ransomware WannaCry, http://www.hitachi.com/hirt/publications/hirt-pub17008/index.html