Cybersecurity Basics 1

Decision Point Cards

Decision Point Card 1:

What Happened: In December 2015, 14 people were killed, and 22 others were injured in a terrorist attack in San Bernardino, California. The attack took place at a Christmas party at the county's department of public health. Two individuals at the party opened fire on those in attendance and left three pipe bombs in the building, which did not explode.

As part of its investigation, the FBI recovered one of the shooter's cell phone, an iPhone 5C, but was unable to unlock the phone due to the high level of encryption. The FBI asked Apple Inc., the maker of the phone, to create a new operating system that would disable certain security features so that they could access the data on the phone. Apple declined, stating that it had a corporate policy to never undermine the security features of its products.

The FBI then asked a U.S. magistrate judge to issue an order compelling Apple to comply with its request. Apple appealed the order and issued a lengthy letter to its customers explaining its stance.

Decision Point #1: Should Apple comply with the FBI's order to create software that would allow the FBI to crack the iPhone passcode?

Decision Point 2:

What Happened: While the legal battle continued, the FBI made contact with skilled hackers across the country. Some hackers even reached out to the FBI with possible solutions. The FBI eventually offered a one-time fee of about one million dollars to a hacker who could help them open the device.

Decision Point #2: Should the hacker agree to help the FBI crack the passcode?

© 2019 GSUSA. All rights reserved. Not for commercial use. This material is proprietary to GSUSA and may be used, reproduced, distributed exclusively by GSUSA staff, councils, Girl Scout volunteers, service units and/or troops solely in connection with Girl Scouting.

Decision Point Card 3:

What Happened: On March 28, 2016, the FBI withdrew from the legal proceedings, announcing that it had unlocked the phone with help from a third party. This third party presumably found and exploited a previously unknown security vulnerability. That means that the iPhone has a weak point, that other black-hat hackers could use for more malicious purposes against Americans. The FBI could choose to release the data to Apple, so they can fix the weak point. But, if they did that, then the FBI might have a harder time accessing iPhones in future investigations.

Decision Point #3: Should the FBI release the security vulnerability data to Apple?