Case Study 2

Name

Institution Affiliation

Proposal for Statistical Research Project/Social Issues: Bullying

With the advancement of globalization, has been a consequent development of cyber-crime cases that are a daily occurrence in life. Crime is comprised of actions that violate existing laws and policies. Most assert that there is a simultaneous occurrence of criminology and crime since they accompany each other. All countries have their set of protocols on the counteracting of such violations. The most vital factors that are considered in handling offenses incorporate the extent and nature of the crime committed. Countries that are affected by high rates of crime rarely progress economically since these crimes have an adverse impact on the national economy. In this modern period, characterized by rapid advancement in science and technology, most countries have to face the complexity that characterizes cyber-crimes. These offenses comprise actions such as identity theft, cyber-attacks, online fraud, cyber-bullying, online child sexual abuse material, and email phishing (Brenner, 2012). This paper intends to explore the hacking crimes committed by Alexey Ivanov and Vasiliy Gorshkov, Russian nationals lured into the United States for employment only to discover it was a setup by the FBI.

Alexey Ivanov started his hacking pursuits targeting U.S. enterprises claiming that he had failed to secure formal jobs in 1999. Vasiliy Gorshkov had founded an organization in 2000 where Ivanov was among the beneficiaries (Pompon, 2017). However, for a brief period, Gorshkov declared his bankruptcy. Ivanov saw this as an opportunity of luring Gorshkov into hacking persuading him that it was an efficient way to netting wages. Among the American businesses that were affected by their activities was the Jon Morgenstern's E-Money Inc. Gorshkov and Ivanov hacked the organization through email threats insisting that the institution's security has been breached (Pompon, 2017). As a result, they claimed, they were the only one that could be able to save the business from financial damage. The two requested that

the corporation provide them with a ransom of $500,000 to ensure its immunity from any current and future hacking incidences (Pompon, 2017). As arbitration for the proper amount was being ensured, E-Money Inc.'s president pursued assistance from the FBI leading to the enticement of the hackers to the United States for alleged rewarding employment. Gorshkov and Ivanov were confident that the new opportunity would give them a chance to abandon their illegitimate activities (Pompon, 2017).

With increased assistance from the FBI, E-Money Inc. brought Alexey Ivanov and Vasiliy Gorshkov into the United States for lucrative employment. When the two were confined, the FBI went ahead to access their computers in Russia and discovered substantial information confirming their activities including nearly 35,000 credit card numbers owned by E-Money Inc. The FBI was appropriately conducting themselves within the roles assigned to them at the national level. It is tasked with exploring complex cyber-crimes in the country, and this comprises cyber-breaches (Brenner, 2012).

Title 28, section 533 of the U.S. Constitution gives the FBI the power to probe and implement federal law violations (Brenner, 2012). Moreover, the national approach ensuring cybersecurity pronounced by the Office of the President provided the FBI the support it required for conducting its operations efficiently. Consequently, the FBI is granted the task of managing national security at the international and domestic levels (Brenner, 2012). Moreover, Russia and the United States were G8 members. The two countries had established an accord that was intended to tackle cyber-violations. With these aspects taken into consideration, it becomes evident that the FBI had complete support in conducting the inquiry into the Russians' breaching activities. It is justifiable to conclude the actions of FBI are not subject to probing under existing U.S. cyber policies. Their actions should be scrutinized because the FBI has been constitutionally

mandated to have unsanctioned access to tools applied in violating cyber-laws for law-enforcement at the national and global level (Brenner, 2012).

A scenario that can be liked the Gorshkov and Ivanov predicament is the Gary Mackinnon case. A Scottish national, Gary Mackinnon was accused of breaching NASA (The National Aeronautics and Space Administration) and the United States Defense Department. Mackinnon confessed to committing the violations that he was charged with, stating that he honorably committed this crime in his pursuit to uncover considerable information concealed from the public (BBC, 2012). In Mackinnon's perspective, he was an individual increasingly motivated to reveal concealed information concerning zero-point energy, antigravity, and UFO-associated advancements (BBC, 2012). He was certain that the public has the right to have access to such information. Still, his circumstance was different since his home country differed with the U.S. administration's intention of extraditing him (BBC, 2012). As a result of this disagreement, Mackinnon case was suspended.

The court had ruled that Alexey Ivanov and Vasiliy Gorshkov contravened the policies that were applicable internationally. Consequently, via the U.S. Patriot Act, the judicial system included the scope of cyber-violations to incorporate online abuse and computer fraud (Brenner, 2012). Thus, the act permitted the probe to include devices in the country and globally.

Overall, cybersecurity is a significant concern for most companies in this modern age because the breach of data and operating systems contribute to considerable losses in revenue. As a result, comprehending the technicalities of information security should be strongly emphasized by all companies susceptible to attacks. Specialist propose various practices that if effected would guarantee the safety of computer systems, thereby countering cyber-crimes. Among the most important practices is the security of passwords involving confidential data.

This method can minimize the chances of intrusion by malicious hackers. Moreover, users should apply the utilization of secure firewalls by enabling and configuring them to address possible breaches. This procedure would protect computers from malware that intends to manipulate unpatched systems increasing their vulnerability to security risks.

References

BBC. (2012). Profile: Gary McKinnon. Retrieved from http://www.bbc.co.uk/news/uk-19946902

Brenner, S. W. (2012). Law, dissonance, and remote computer searches. *North Carolina Journal of Law & Technology*, *14*(1), 43-90. Retrieved from http://scholarship.law.unc.edu/ncjolt/vol14/iss1/4

Pompon, R. (2017). Russian hackers, face to face. Retrieved from https://f5.com/labs/articles/threat-intelligence/cyber-security/russian-hackers-face-to-face