Ethical Challenges – Cyber

From Security Intelligence (written by Aidan Knowles) 12th October 2016

Hollywood Hacking and Real-World Challenges

In the very first episode of "Mr. Robot," the Emmy-nominated, cybercrime-themed fictional television series, the show's protagonist, Elliot, a disillusioned cybersecurity engineer working in New York, faces a critical ethical decision on the job. The character, played by Rami Malek, comes across a suspicious file on a client's compromised server when diagnosing a distributed denial-of-service (DDoS) attack. This unusual file has a mysterious message for Elliot: "Leave me here."
In this pivotal moment of the show, Elliot can choose to either delete the file (the ethical decision) or leave it on the client's server. Intrigued, Elliot acts unethically and leaves the file on the server without notifying his incident response team, management or the server owner. This decision is the catalyst upon which the whole story arc hinges, leading to the protagonist's involvement with the enigmatic illegal cybercrime gang fsociety and a massive data breach for the important client.

While the depiction of cybersecurity ethics in "Mr. Robot" is a somewhat overdramatic Hollywood rendition, it is not totally dissimilar to the real-world ethical challenges security professionals frequently encounter in the field. Through both deliberate and unintentional actions, a cybersecurity professional can criss-cross the often complex and delicate ethical line. Like Malek's character in "Mr. Robot," even the smallest diversion in the nuances of ethical decision-making could open a can of worms with far-reaching consequences, potentially putting the business, customer base and individual at risk.

Hacking Airplanes: Helpful or Harebrained?

Security researcher and One World Labs founder Chris Roberts made controversial headlines in 2015 after tweeting that he was considering doing a live penetration test of his domestic United Airlines flight to Syracuse, New York. Roberts, who was the subject of an FBI affidavit, allegedly commandeered a Boeing aircraft by tampering with the thrust management computer via its in-flight entertainment system, causing "one of the airplane engines to climb, resulting in a lateral or sideways movement" of the aircraft, Wired reported.

It's unlikely Roberts intended to threaten or harm himself, airline staff or the other passengers onboard. Despite apparent white-hat intentions, however, the consequences of Roberts' alleged actions against such critical systems could have been grave.

After the story broke, several prominent cybersecurity professionals spoke publicly about the dubious ethics and legalities at play. According to Business Insider, Alex Stamos, then CISO at Yahoo, tweeted, "You cannot promote the (true) idea that security research benefits humanity while defending research that endangered hundreds of innocents."

Education, Awareness and Outreach

While a deeply integrated code of cybersecurity ethics and conduct is vital, it is also crucial to cultivate ethical teachings among students and young enthusiasts — the security professionals of tomorrow. By promoting awareness of cybersecurity ethics at the early stages of learning and professional development, we can help ensure that future white hats stay on the right side of the ethical divide.

Bug bounties and hacking competitions provide ethical sandboxes where budding young hackers and senior professionals can mess around and challenge themselves. Many major organizations, including Facebook, Google and several prominent airlines, offer crowd-sourced bug bounty programs in which hackers are rewarded for discovering vulnerabilities in selected targets. This model improves the security of the company's assets while offering a defined structure and guidelines under which eager global security researchers can legally hack, learn and reap handsome rewards.
Cybersecurity enthusiasts can also use a variety of deliberately vulnerable simulation platforms to learn penetration testing skills inside a safe environment. It is important that such education tools provide users with the necessary ethical context to ensure that their teachings are not misplaced.

Who's to Blame?

Young rogue hackers often fall into the hands of law enforcement when conducting activities against legitimate, unsuspecting targets. Many plead ignorance, asserting that they did not realize the activities were illegal.

Who is to blame in these situations? In some cases, hacking tools, including those that contribute to DDoS botnet attacks, are part of the problem. Often, at a core level,

this software has become so easy to use that it enables unwitting newbies to invoke potentially illegal damage across the internet with just a single mouse click.
On the other hand, many hackers have knowingly crossed ethical boundaries with ignorance falling short as a defense. If a young cybersecurity enthusiast behaved unethically in his or her juvenile hacking past but shows a promising future, can he or she be trusted by a potential employer? Despite the noted demand for cybersecurity professionals, organizations are usually hesitant to hire talented ex-black hats.