**Chapter 10**

*Criminals and Crimes*

Criminals, such as hackers or crackers, have become a major threat to the movie production industry. There are different reasons why hackers hack into a company. Some hackers are current or former employees that use their position to steal sensitive information for industrial sabotage and for personal gain reasons. Other hackers utilize their skillset for criminal intentions. Finally, a minority of hackers/crackers just snoop around without malicious intent. These hackers have become a problem in the movie production because companies run the risk of their intellectual property or financially records being compromised. Recently, Netflix, Sony, and Home Box Office (HBO), have been victims of cyberbullies that have stolen their intellectual property which resulted private information being publicly released.

*Cyber Terrorism and Piracy*

Cyber terrorism is the act of criminals using a computer to cause fear in society. The movie industry is particularly vulnerable to cyber terrorism. In November 2014, Sony was hacked by a group that called themselves Guardians of Peace (GOF). During this hack, skulls would appear on the computer screens of users; this caused chaos and panic across the industry. This hacker group exposed sensitive information, such as social security numbers and salary benefits, to the public. Furthermore, at least 5 films were released to the public through file sharing, which violated copyright infringement protections.1,2 As a result, Sony production experienced a loss of revenue with the release of these films. ‘Fury’, which was not yet released in theaters was being pirated; the film was found that approximately 888,000 different IP addresses downloaded the content. At the time of the data breach, this was one of the second highest films being downloaded. Likewise, ‘Annie’ was another film which fell victim to hacking which had been pirated 3 weeks before the film was to be released in theaters.1,2,5 Lastly, another Sony production films that was hacked and had issues with the release was ‘The Interview’. GOF threatened many cinemas to an act of terrorism if the film was to be released in their theaters. They further threatened Sony production that top secrets would be exposed if they moved forward with the theatrical release.1 Sony production was left with little alternative and had to pull the film from theatrical release. Piracy is a huge threat in the industry as it causes the film to lose potential revenue from box office sales.

*Managing Information System Security*

Management of company security within their information system is crucial. These companies must account for different security vulnerable events such as natural disasters, employee error, foreign travel, and outside cyber security hackers. When taking precautions in the security of the information system, the systems security team will assess the risk, develop a security strategy, implement systematic controls and training, and, finally, routinely monitor the security system. This is highly important especially if the company has already been a victim of cybercrime. For example, it is reported the HBO has been a victim of the largest cybercrime with approximately 1.5 terabytes of data taken from this crime. The data includes scripts, financial documents, company emails and customer information. It is important note that HBO increased their cybersecurity, so they will not be prone to another cyberattack.3

*Developing a Security Strategy*

When a company is trying to upgrade their cybersecurity, the most effective way to do so is by considering three different control systems. *Preventive control* tries to prevent any negative event from occurring; this could be done by ensuring that users are only allowed to access what is needed to perform their duties and restrict them from accessing other information that is not within their jurisdiction. *Detective control* is done by evaluating and determining if there was a breach in the cyber security. The last system is *corrective control* which focuses more on acting after the compromise has accrued and restoring the compromised data. It is important for the company to have a disaster recovery plan in case a problem arises, such as having a backup site. This is important because as we’ve seen before in production industries such as Sony, Netflix, and HBO, when there is a breach in their informational system sensitive information is release making the individual prone to potential fraudulent crimes. Cybersecurity can easily decrease the likelihood of any further threats to the company’s information system by taking preventative and corrective action to realize where the weaknesses lie in the company cyber security systems.

1. The Interview: A guide to the cyber attack on Hollywood. <https://www.bbc.com/news/entertainment-arts-30512032>. Accessed March 3, 2019
2. Hollywood's hacking pains are bigger than movie leaks. <https://phys.org/news/2017-08-hollywood-hacking-pains-bigger-movie.html>. Accessed March 3, 2019
3. HBO Hack Could Be the Biggest Industry Hacking Ever — Everything You Need to Know<https://www.indiewire.com/2017/08/hbo-hack-details-fbi-investigation-sony-biggest-history-1201862895/>. Accessed March 2, 2019
4. Sony’s New Movies Leak Online Following Hack Attack. <https://variety.com/2014/digital/news/new-sony-films-pirated-in-wake-of-hack-attack-1201367036/>. Accessed March 3, 2019