Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

3 Important Cybersecurity Lessons Learned From 'Star Wars'

(January 27, 2016, 11:02 AM EST)

Growing up in the '80s, I watched "Star Wars" (we never called it "A New Hope") over a hundred times. It was and still is my favorite movie of all time. While I loved the action, I didn't realize that I was learning valuable lessons for a later career in cybersecurity. Below are three cybersecurity lessons from the original Star Wars movie.

Lucas Amodio

1. Don't Pick Up Every Piece of Junk You Find

The Death Star, the Empire's greatest technological terror, finds a piece of junk floating in space, the Millennium Falcon. The Empire picks the Falcon up in its tractor beam and brings it on board past all of its defenses. Once it is on board, the Empire performs a scan of the Falcon to see if it is occupied. The Empire reads the Falcon's logs which say that the crew abandoned ship soon after takeoff. The defensive measures, stormtroopers, leave the ship and allow a scanning crew to enter the ship alone. Of course, we all know what happened next.

So what could the Empire have done differently? First, the Imperials could have left the Millennium Falcon floating in space and not picked it up. Like memory sticks that you find in the parking lot or spam emails, don't pick the stick up, don't open the email, don't click on unknown links. Second, the Imperials could have scanned the Millennium Falcon before they brought it into their facility. Have a virus and malware scanner that checks all of your emails and all of their attachments. Set-up the scanner so that it scans them before they are delivered to your mail program on your computer.

Third, the Imperials could have quarantined the ship while it was being scanned. Have a spam filter setup to quarantine suspicious emails. If you have to look at the memory stick, but aren't sure about it, then open it on a computer that is not connected to the network; one that can be erased if it becomes infected. Fourth, the Imperials could have dug deeper into the logs before believing exactly what was stated (that the ship was unoccupied). Don't believe what the links or email addresses state because they can be spoofed. Put your cursor over the link or address and see if it matches. Call the sender to verify that the email is from them.

2. Looks Can Be Deceiving

While running around the Death Star, Han and Luke dress up as stormtroopers escorting a prisoner. As they travel around the Death Star, they are believed and not questioned. The system even allows them to reach a secure area, Detention Block AA23. The Imperial officer does not allow them to enter the detention block and sends troops to secure them and their prisoner while he clears it. After Han and Chewie shoot up the detention block, Han tries to convince those on the other side of the intercom that everything is fine. However, Han does not say the right things and the officer on the other side of the intercom asks for his authorization and operating number, and sounds the alarm when Han doesn't respond.

In this case, the Empire did pretty well. They could have put some type of access control on the elevator so that it wouldn't give access to the detention block without the proper credentials. Much like putting a password on a computer, network or file to restrict access. However, the Imperial officers did perform their security duties well. They questioned what was presented before them, and did not take it at face value. Even though there were two stormtroopers with a shackled prisoner, the officers asked for further authorization.

For example, just because someone is in the facility doesn't mean that they should be able to log onto a computer. Even if they are in the server room, they should be asked to show their badge. They should be required to use their own credentials to log in. If something sounds weird, like Han's comment, "How are you?" then you should check for their authorization. Just because the person on the other end of the phone says that they are from information technology, doesn't necessarily mean they are. Same if the "IT" guy shows up to update your computer. And if you see someone that you don't know walking the halls, check for their badge. If you don't see it, then ask them for it, and ask who they are. If you don't get a good answer, follow up with someone who should know that they are walking around.

3. Segment Your Network

After narrowly escaping the stormtroopers in the detention block, the rebels find themselves in a trash compactor. The trash compactor starts to close in on our intrepid heroes to squash them flat. However, Luke is able to reach out to R2-D2, who plugs into the network and stops the compactor. He even opens the door to let them out. R2 is able to access the Imperial computer through the hangar bay. It is even hinted in "The Force Awakens" that he is able to download Imperial databases, while he is connected to the Death Star computer network.

In this case, the Imperials had interconnected their network so that computers in the hangar bay could access systems on the detention level. We saw earlier that R2 was able to discover that Princess Leia was on the Death Star, where she was being held, and that she was scheduled to be terminated. He was then able to access and control machinery and doors on the detention level to assist his companions.

Computer networks, especially those with classified data, should be segregated out so that if someone breaks in to access one type of functionality, the intruder can't also access other functionality. After all, someone who works in the hangar bay has no business accessing the detention level, and vice versa. Once an intruder breaks in, they should not have free reign. This is how the Target hack happened. Once the intruders got in, they were able to access anything.

Bonus: Always Have Multiple Backups

In "The Force Awakens," Kylo Ren is looking for a missing map that is supposed to be on BB-8. He captures Rey, who has seen the map because he believes that he can get the map from her memories. Once he has her, he calls off the search for BB-8. However, it turns out that he can't access her memories, which means that he can't access the map.

You should always have multiple backups, sometimes even in multiple formats. Kylo made the classic mistake of only relying on one copy of the data. However, when it turned out that the data was on an incompatible format and could not be read, Kylo was out of luck. First, always make backups of data that you need to keep. Second, make multiple backups. Sometimes backups become corrupted, which means if that was the only copy, then the data is lost. Third, look at backing up data in multiple formats. Sometimes, the backup that you need to access is multiple years old. It might even be in a format that is no longer supported. If it is in more than one format, there is a better chance that at least one copy will be readable in the future.

I look forward to the next "Star Wars" movie "Rogue One," which is expected to come out next December. It is rumored to cover stealing the original Death Star plans and it should have even more cybersecurity dos and don'ts.

—By Lucas Amodio, Armstrong Teasdale LLP

Lucas Amodio is an associate in Armstrong Teasdale's St. Louis office. He is part of the firm's intellectual property practice group. The majority of his practice focuses on high-technology and computer-related matters involving patent law and cybersecurity. Amodio is also a Certified Ethical Hacker (C|EH).

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.