Technical Brief  
CYB 200 Cybersecurity Foundations

Sergio Mateos

Southern New Hampshire University

I’m a government employee, who work with the United State Army top secret military contracts. At the time I arrived at work, Jan, a work college that I know from college, started working in the same space. Since I have known Jan, she has always been having financial problems, but lately I notice that Jan has been coming to work with nicer clothes and expensive jewelry. At first, I didn’t pay attention but a couple weeks ago, I noticed that Jan has been bringing her tablet to work. At work we have a strict policy about bringing devices, so I approached her to remind her about the policy to keep her out of trouble and she responded, “I use it to read the newspapers”. Later the same day, I went to Jan office asking for an upcoming project, and I notice she was taking picture from her tablet. I confronted her but she gave me excuses about how she was behind the project, and she needed to cat up at home. I mentioned this situation to my supervisor, and they started an investigation. The pictures that Jan was taking were uploaded to a cloud.

Jan has matching up her action with the characteristics of an insider threat actor, first she has access to the top-secret military contracts, which just couple people are available to access, a usual insider tries to reach the most deeper and advance level possible. Second, she started wearing expensive clothes and jewelry, which indicates that whether reason she is selling the information is for financial gain. Third, Jan took pictures with her tables in which she established that she only used for reading the news and uploaded to a cloud storage.

Insiders have a lot of potential to hurt a company or institution since they are acting like employees to be able to have access to important information. In our scenario, Jan detected since I been aware about attack that an occurrence even with employees of the government agency. Since I know Jan, I can have developed a friendship with Jan, I can understand her financial situation and when she started wearing expensive clothe and jewelry I was impressed since I know how she is been struggle with money. But what helped me realize what her intension was that she was taking pictures of projects when first at all we weren’t supposed to have any device at work. Jan was easily detected by mapping her path and ended up of her uploading the picture into a cloud. Being aware is the best practice for insiders since people may know them but they are looking to harm the company.

Jan will face many legal issues since she stole top secret information for financial gain. Jan broke the agency police device in the building, since they are working for United Stated Army, there is no tolerance for people who decide to break their policies, which end up on termination. Jan decides to take pictures of an important project and after mapping the path of her decision, the pictures were found in a cloud storage, this is data theft, which is violation of the legal; system and will. Face penalties and even time in jail since the information was used for financial gains. Finally, the reputation of Jan would be null, since she broke the trust of the company she worked for, it would be hard for another agency or company to trust her.

Since Jan was identified as the threat actor (insider), the security team needs to analyze what type of projects she works on so we can have better understanding. In our scenario, I respond correctly to always be aware of my surroundings, pay attention to what people are doing, and always report to the supervisor if there is any question. After Jan was identify as an insider, the security team will implement a risk management plan to mitigate Jan, first train the employee about cybersecurity awareness, second minimize access control to Jan, so she cant leak more data, third identify organization assets and prioritizing risk,