The Ashley Madison Hack & The CI Implications It Could Bring To Light

- San Diego ISAC Counterintelligence Sub-Committee - October 2015 -

-Photo of the Ashley Madison sign-on screen-

So, you know an employee who knows a guy whose long lost uncle's name showed up on the Ashley Madison hack list. This employee of yours has approached you as a favor because he's wondering what to do about it. Is it reportable for an individual who has current eligibility and access? What would your response be?

Before addressing those questions, let's get some background and then we'll examine the issues from an industrial security perspective.

The Ashley Madison hack that reportedly occurred in July of this year was a data dump posted to the dark web using an Onion address. The dump includes account details, log-ins (yes, over 120,000 users chose to use 123456 as their password) and seven years of payment transaction details of approximately 32 million users of the site, which is advertised as a site for married individuals seeking partners for affairs. (Zetter, 2015)

Information in those records could include: names, street addresses, email addresses and amount paid, but not full credit card numbers. In fact, each transaction includes four digits, which could be part of a credit card number, or it could be a transaction number. 91,000 accounts were based in San Diego (Baker, 2015), though it's impossible to verify whether fake information was used in any single account.

While the authors of this article are not federal adjudicators on national defense matters, we believe that reviewing federal regulations concerning the 13 adjudicative guidelines may shed some light on the issue. Guidance regarding: sexual behavior, personal conduct and outside activities play a key role in defining the subjectivity in:

- Coercion, exploitation, or duress
- Behavior that reflects lack of discretion or judgment
- Conduct that raises questions regarding judgment, untrustworthiness, unreliability and lack of candor

From a NISPOM adherence perspective alone it is recommended that an FSO review ISL 2011-04 which provides the following definition of adverse information:

> *"Any information that negatively reflects on the integrity or character of a cleared employee…"*

Now that we've covered the personnel clearance side, let's look at some of the CI possibilities. Regulations and policies aside, a honey trap[1] (known by some as a honeypot) has proven to be a highly successful method of coercion in relation to espionage practices. Today's technological culture has vastly increased the risk of an individual falling victim to the honey trap method (as well as a myriad of others). This increase is then multiplied when taking into account the number of apps and websites available that are intended for similar purposes as the Ashley Madison statement on their sign-on screen, "Life is short. Have an Affair"

For an individual who utilizes these platforms, while maintaining access to sensitive information, it could be compared to a mouse jumping into a pit of snakes. Sooner or later the risk of being eaten increases as the snakes fail to obtain information through other means. As such, a critical vulnerability has been reflected which could be easily utilized for malicious intent.

Whether you are the only (or one of many) Industrial Security Professional at your organization, you should be comforted by the fact that most scenarios can be analyzed by utilizing a basic risk management theory (*see Figure 1*).

Since the website itself and the hack that has been uncovered could be viewed as the vulnerability, evaluating the particular asset(s) that the employee is/has been working on is a good place to start. Talk to the PM's to become more familiar with the asset's and identify key elements that (if compromised) would result in disaster.

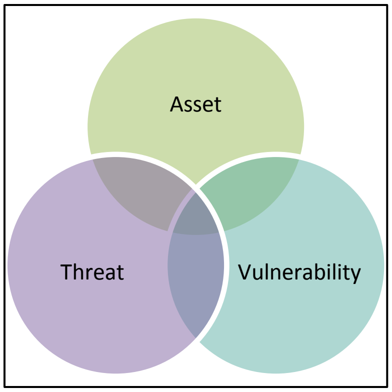

Figure 1: Risk Management Theory

[1] : A "Honey Trap" is defined as a strategy whereby an attractive person uses his/her powers of seduction to coerce someone into doing or revealing something. (Dictionary.com, 2013)

The threat could equate to rival corporations (both foreign and domestic), or foreign intelligence services that are willing to obtain the identified asset (or information concerning it) through malicious actions. This information could come from open source analysis, but a request to your local intelligence community POC (DSS, FBI, NCIS, etc.) will provide you with the most accurate results.

It's only after you review all three of these collected elements, that accurate determination of the true risk can be accomplished. A good example being if the employee has an account which has been compromised, works on a program that is a critical advancement in US military strategy and proof of foreign attempts to gain information concerning said program have been provided to you. In this example, heightened communication of that risk should be made to both the PM and DSS/FBI due to NISPOM 1-301.

Purely having an account with an online special interest group is not reportable. Having an affair could or could not be viewed as something that is required to be registered. Given the intention and personal nature of the website, it can be argued that there are blackmail/coercion/questionable judgment possibilities. Because of this, it's a good idea to remind employees that all blackmail and coercion efforts of any kind must be reported to security.

Back to how to respond to the employee asking the question for his friends long lost uncle. Obviously you should at least try and give them advice instead of letting them know that you'll be looking into measuring the risk to their program(s). Maybe use the following information in your initial response? At this time, the disclosing of personal account information and the possible credit information is significantly more important from a security perspective than the company that was hacked. This "uncle" may want to initiate the following standard personal investigations:

- Identify what information was revealed – Social Security numbers, credit card numbers, driver's license and other identification numbers.
- Place a fraud alert and order credit reports.

The Federal Trade Commission has published a guide for possible victims of identity theft:

https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf

Because it's in the news, questions will undoubtedly arise and it's important to be prepared to answer. Replying with, "I don't know" is rational since this area of concern may be viewed in a subjective manner. However, it is highly recommended that your points of contact in the intelligence community receive a request from you concerning any known threats surrounding the asset identified through the risk determination process. You may be surprised what you discover!

So what's for sure? The first and foremost lesson that should come from the Ashley Madison hack is that no matter how secure you think personal information is, it isn't. There's no such thing as "Private" on the internet. ALL the hacks that have been recently publicized (Target, Sony, Home Depot, etc.) should be proof enough that any personal or program information is, at the very least, not as secure as we may have thought a couple years ago.

The result? Not only should we be more vigilant in examining the things we have at risk online and in our lives, but also about the people we place on government and corporate sensitive programs.

Bibliography

Baker, D. (2015). *The San Diego Union Tribune*. Retrieved October 2015, from http://www.sandiegouniontribune.com/news/2015/jul/20/ashley-madison-cheaters-website-hacked/

Dictionary.com. (2013). *Dictionary.com*. Retrieved October 2015, from http://blog.dictionary.com/espionage-terms/

Zetter, K. (2015). *Wired*. Retrieved October 2015, from http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/