YOUR SAFETY AND PRIVACY ONLINE

THE CIA AND NSA

SIGGI BJARNASON

Your Safety and Privacy Online

The CIA and NSA

Siggi Bjarnason

This book is for sale at http://leanpub.com/onlinesafety

This version was published on 2019-09-09

ISBN 978-1-7333068-0-5

Library of Congress Control Number:2019910732

Contents

1. Disclaimer

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/onlinesafety.

2. About This Book

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/onlinesafety.

2.1 About the author

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/onlinesafety.

3. Introduction

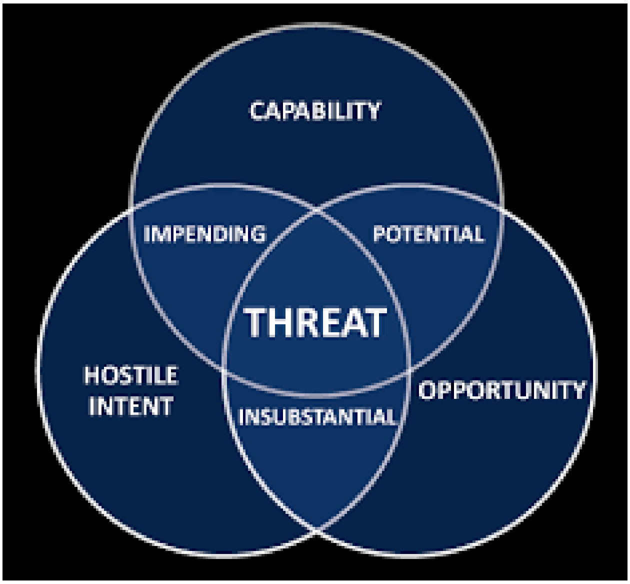
This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/onlinesafety.

4. General Principles

I am going to start by going over some general principles before I get started. Give you some foundation you can leverage, as you start on your online security journey.

4.1 Threat Modeling

The first thing I need to discuss is the concept of threat modeling. Threat modeling is the action of deliberately thinking through and cataloging potential threats in your everyday life. “Threat landscape” is another term used in this context. These terms come from the idea that you can create a model or a landscape picture of all the things that are a threat to you. This picture illustrates well the concept of a threat:



Definition of a threat

Let us discuss this picture a little and unpack all the wisdom in it. At a high level, it is saying that for something to be a threat, you need to have three ingredients. For those that are avid crime mystery readers or like to watch crime shows on television will recognize these ingredients. These ingredients are intent, opportunity, and capabilities. Crime TV shows, often label intent as a motive. Without all three elements present at the same time, you have no real threat.

The term capability refers to having the ability to do something. This ingredient is present in the majority of cases involving threats to our physical well being. Most of us possess the physical ability to do unspeakable harm to each other. Luckily most of us are a decent human being and could never even imagine harming another person. In other words, we lack the hostile intent to do each other harm. Going back to the term capability, when it comes to online threats, this element is frequently missing as you require a good deal of technical know-how to be a menace online. So those without technical knowledge lack the capability to be a threat online. So regardless of how much they desire to be a menace, they can never become a real threat online until they gain the required technical know-how.

Opportunity is the concept of having access to something. It's about being in the right place at the right time and with access to the target. In the physical world, this means having access to the person you wish to harm. Personal bodyguards, diplomatic protection details, etc., rely heavily on removing an opportunity from the equation to keep their protectee safe. They can't control people's intent, nor can they control people's capabilities; however, they can manage people's opportunities. As we discussed, there is no threat without all three components. By strictly control public access to their protectee, they strictly limit the opportunity factor, thus limiting the threat and the risk.

The last element is the concept of intent, sometimes also called motive or desire. If folks have no ill will towards you and do not wish you any harm, they possess no threat to you. Going back physical protection methods, bodyguards and such, the concept of security screening deals in this space. Security screening tries to assess if you hold any ill will against those being protected. This can be very hard to determine and can flip around without any notice or warning. We see this when a seemingly peaceful place all of a sudden becomes a hotspot of violence. In most cases, the folks involved didn't suddenly gain new opportunities or obtain new capabilities. Most of the time, something happens to trigger the mass of people to suddenly gain newfound desire and motivation to rise up and take things into their own hands.

As you see in the Venn diagram, the following situation occurs when one of the elements is missing:

- Opportunity + Capability = Potential Threat
- Opportunity + Hostile Intent = Insubstantial threat
- Hostile Intent + Capability = Impending threat
- All three = actual threat

As you may have observed, this is a very fluid concept; all three concepts can change without notice and change your risk instantly. You may only have a potential threat because the intent is missing, then something happens, and a friend becomes a foe, and now there is intent. Someone may not have the capability, then they learn a new skill, and now they have the capability. There may not be an opportunity one moment, then the next moment an opportunity pops up.

Then there is the concept of vulnerability; I think this one is somewhat self-explanatory. In the physical realm, we are all vulnerable to physical attacks like being shot, stabbed, or just beaten. Some are more vulnerable than others, depending on each person's self-defense capabilities. I think it is safe to say that all humans are vulnerable to gunshots regardless of your training. Protective gear, such as helmets and bulletproof vests, can reduce that vulnerability to some degree. Also faulty protective gear, such as a bullet proof vest that doesn't really stop bullets, gives you false sense of security and leaves you vulnerable.

Now extrapolate this into your online world, depending on your training, condition, and protective gear, you have particular vulnerabilities online. The goal of this book is to up your training and introduce you to protective gear so that you can reduce your online vulnerabilities.

The last big concept when it comes to threat modeling is the concept of risk. Risk can be expressed mathematically as the multiplication of threat and vulnerability. That is the higher either the vulnerabilities or the threats are, the higher your risk is. If both are high, your risk is significantly higher than if just one is. I'm very mathematically inclined, but I know that not everyone is, so let me lay out some basic multiplications to illustrate this:

- 1 x 1 = 1
- 1 x 5 = 5
- 1 x 10 = 10
- 5 x 1 = 5
- 5 x 5 = 25
- 10 x 1 = 10
- 10 x 10 = 100

The lower your risk is (the number after the equal sign), the less of a chance you have of becoming a victim. There is no such thing as zero threats or zero vulnerabilities and thus no such thing as zero risks. In other words, you can have an exceptionally low risk, but you can never have absolutely no risk.

Because of how fluid the concept of threat is, your threat model will be equally fluid and thus required frequent re-evaluation. So now, back to the idea of a threat model, also called threat landscape or threat analysis. Just a footnote, in the world of threat intelligence, these words have a slightly different meaning; however, for our purposes, they are close enough to be the same.

So how does one create this threat model you ask. All you do is think through all the possible things you feel are a threat to you. You don't have to justify what you come up with to anyone, this can be based on gut feeling, intuition, experience, etc. You may want to keep this to yourself and not sharing it with anyone. If you do share it with someone, and they call you paranoid, that can be a good thing as it indicates you've taken this seriously. This will end up being a very individual and personal model and can be influenced by so many things. It is an informal thing you do for yourself, whether you write this down or keep it in your head is totally up to you.

For an example of how threat models change from person to person consider this. In general, women will have a completely different threat model than men do. For women 100's of everyday tasks, from getting gas to buying groceries, include a wide range of threats to their wellbeing. Typically, men don't have to worry about those things.

Here is another example of how a threat model can differ from one person to another. Think about a dissident living in China, Russia, or any other country where the government doesn't appreciate being held responsible for their action. This person will most likely have a very complex threat model. Now for contrast, let's think about a person that lives in a country where free speech is protected. This person may have an ordinary, maybe even dull, job and aren't involved in much beyond perhaps a bowling league. That threat model is likely straightforward by comparison and starkly different.

Here is some more food for thought on the concept of threat model and how they can vary significantly from person to person. For each of these, the opposite is "others, not so much."

- For a large section of the population being roofied by a

random person at a bar is a real threat to their safety. Some might say this could affect as many as 40-50% of the population
- Some folks are concerned with getting hacked by a random hacker, especially if they are attending a conference popular with hackers.
- Some people truly and honestly believe that anyone using any product made in China, whether it is software or electronics is absolutely certifiable insane.

None of these folks are wrong, it is all a matter of perspective, personal situation, background, etc. Based on what I have read and heard about, being roofied is the most significant danger to the largest population of the threats listed above. All of them are real threats to different folks. That is how personal and varied threat profiling can be. The big thing to keep in mind is that just because something isn't a threat to you, doesn't mean it isn't a threat to someone else, and vice versa.

Speaking of China, there has been a fair amount of news lately on a company called Huawei and the Chinese government. Let's use the Venn diagram above to analyze some of that news.

- Is the Chinese government capable of spying anyone they wish? Absolutely, I do not doubt their capability in that regard.
- Do they have the opportunity to spy on anyone they want? There is a very high probability they do. Those that believe anyone who uses Chinese products is insane, certainly would argue that they do. For the record I believe they have a very compelling argument. I would

even say that if they wanted to spy on you, they probably could do so even if you only use products made in the US.

- Do they have the intent to spy on everyone in the world? Unlikely. Are there billions of folks, especially Chinese citizens, and others who oppose them, being spied on by the Chinese government. Absolutely, no doubt about it. Are they spying on US Citizens? Very likely.

As you see who you are, where you've been, where you are from, and what you do, are amongst others, all factors in influencing your threat model. Just because you aren't concerned about something and the person right next to you is, doesn't make either one of you wrong. Debating how someone should be concerned about something you are concerned about but they aren't (or vice versa), is as valid as discussing how someone should love peanut butter because you love peanut butter. For the record, I hate even just the smell of peanut butter, which makes me very much an oddity in the US.

As with all personal matters like that, you can talk about why you are or are not concerned about something, but shaming someone for having a different take on things is never OK just like any form of shaming is never OK.

For you to be effective in your quest to be more security conscious, you need to take the time and really think through your threat model. Think about all the things that could threaten your daily life, and make sure you dig deep. This should encompass both physical threats and online threats. As you work through this make sure you include counter measures, as in how do you respond to those threats. Start with physical threats and then add online threats as you progress through this book. Start with the big stuff, like is there anything in your daily life that threatens your life? Do you live in an area with high murder or assault rates? If so, what precautions do you usually take, how do you deal with that threat? From there, you can branch out into other threats to your way of life. Don't limit this to what could literally end your life that is just a starting point. Include in here as well stuff that could significantly impact your quality of life. This should be somewhat detailed and not high level. Think about who and what could threaten your way of life. For example, getting laid off from work might be on many people's threat model; however, go deeper than that. What are some possible situations that might lead up to you being laid off? Losing your life savings, being assaulted, mugged, etc., are other possibilities for the physical threat model. For each of them go deeper than one or two words. These are examples from the physical world that I imagine most people can identify with.

After reading this book, you will be able to integrate online activities into your threat model as well. A good threat model covers all aspects of your everyday life. It is also iterative and always evolving as I identified above. As I said, a threat model is a highly individual and personal thing that you do to help you gain an understanding of threats in your life. You should never have to justify it, and who you share it with is totally up to you. It is normal and acceptable not to share your threat model with anyone.

4.2 Threat actors

Let us touch on the concept of a threat actor really quick. A threat actor is simply the person or persons perpetrating the threat. For all practical purposes, the term threat actor is a synonym to a criminal, and you may catch me using them interchangeably. This can be a single person but is more often a group of people, such as organized crime families, also known as the mafia. While in the past, the mob has focused on physical crime; they got onto the online crime game several years ago. Here are some common threat actor types.

Nations State Threat actors

Criminal organizations sponsored by a country. Russia, China, and North Korea, amongst others, are widely considered having nation-state threat actors. There are those who even say the United States National Security Agency and the Central Intelligence Agency are nation state threat actors.

Advanced Persistent Threats (APT)

These are highly sophisticated threat actor groups which significant resources at their disposal. Once they select a target, they tend not to stop until they've accomplished their mission. This tends to be either funded by a nation-state, or other organization with deep pockets. Both APT and nation-state groups typically have a particular task which their sponsors gain specific benefits from, often in terms of reputation, revenge or information. If you are targeted by an APT, there really isn't much you can do beyond moving in with the Amish to stop them. Most APT groups seem to not be financially motivated, North Korea being a notable exception.

Organize crime groups

As previously mentioned, these are your classic mafia groups turned high tech. Their motives tend to be simple, money. Their missions are all about either direct financial gain or gaining something that can be easily monetized.

Activists

In the physical world, these are often called Eco-terrorists. They claim they are operating for a higher cause. They tend to attack companies and people they feel they need to teach a lesson. That they can teach them the necessary lesson by hacking them, breaking into their system, stealing from them, defacing their websites with their message, etc.

Random threat actor

These are just individual threat actors that are in it for a myriad of reasons. Some are in it merely for the financial gain, while others are trying to settle a grudge. This could be a disgruntled employee, unhappy customer, or even just a friend turned foe because they felt slighted.

Script kiddies

As the name implies, these are often teenagers or young adults doing stupid stuff because they can. Often, they have no real mission. Some are just after some excitement and seeing what they can do (typical teenage stuff), others are attempting to make some easy money, etc. There is a lot of cross over between script kiddies and random threat actor. The random threat actor frequently is a tad bit more sophisticated than a script kiddy and often have more technical know-how.

5. Just a sample

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/onlinesafety.