

In The Digital Age, Our Data Is Currency

When we analyze a risk of any kind, we need to look at its impact and probability. How bad is it, and what are the chances of it happening to me?

When it comes to cybercrime, we are pretty good at understanding the impacts. We've seen the stories; we've heard the reports, and we know the numbers associated with cybercrime are devastatingly huge.

Where we tend to struggle is truly grasping the probability of a given cybercrime. No one ever thinks it could occur to them. Year after year, people will ask me, "Danny, why would a cybercriminal come after me? I have nothing of value," or "I'm too old," or "I'm just a kid, and my company is too small."

This lack of understanding creates a problem for organizations trying to spread cybersecurity awareness because no amount of information sharing can help educate an audience that just doesn't care about the subject matter you are trying to teach. And they simply can't care about something they believe will never affect them.

That being said, it is my hope this article helps shed some truth on the probability of threats associated with the digital age.

Before I get into that, let's talk about something that I know we are pretty good at protecting, our money. When I was a kid, I pulled some cash out of my pocket at a mall to count. My dad gave me a stern look and said, "Never count your money in public." This was a saying in the 1980s, and I think there is a country song with that same title. If there isn't, there should be. We knew money was valuable, and we knew there were bad people that wanted to get their hands on it. As such, we had to be careful with it.

The value of things like money or currency is determined essentially by the demand for it. How often is it bought, sold, traded or even stolen?

That being said, how come we don't treat our data with the same caution that we treat our money? Not a day goes by that our data isn't bought, sold, traded or even stolen. Yet we willfully give our data away by posting way too much online without a second thought, we blindly click on terms and conditions of free apps without considering what it might mean to our data.

It's important to understand that a cybercriminal doesn't care who you are, how young or old you are, or even much money you have or don't have. They want your data. Data is the newest form of currency, and it is very valuable to a lot of scary people.

Once a cybercriminal has your data, they can sell it on the darknet. What is the darknet? The simplest way to explain the darknet is that it's the digital underground, where criminals can buy and sell all sorts of things, including your data, and it's the last place you want your data to be found.

You may say, "But I have no money. Why would anyone want to steal from me, and if they did, what could they possibly get?" In many cases, cybercriminals don't want your money, but rather your identity, and your data will help give them exactly that.

There are a lot of nefarious people in the world doing nefarious things -- people who would much rather do those things in your name.

To truly understand the probability of danger for almost anything, you need to understand two things: the threat and the vulnerability. For cybersecurity, the threat is simple. Cybercrime is a thriving industry with no slow-down in sight, and there are really two main reasons for this.

Cybercrime is increasing in popularity because it is incredibly lucrative for the criminal and presents minimal chance for physical injury to the criminal. In many cases the cybercriminal does not even have to live in the same country as the crime they are committing, allowing them to easily attack their unsuspecting and unprepared victims.

The vulnerability ties back to what I stated earlier in this article: We are not too concerned with cybercrime because we don't believe we are targets for cybercriminals.

And that is why the first step to understanding cybersecurity safety is to understand you and your data, as well as the data of your colleagues and loved ones, is a prime target for cybercriminals. Always remember the first law of cybersecurity: If you use and have access to data, you are at risk for a cyberattack.

By truly understanding that you are a target to cybercriminals, you have taken a good first step toward better cybersecurity hygiene. From there, it's important to know that most cybercrime centers around your sensitive information. Keeping this in mind, always keep tabs on what information of yours could be considered sensitive -- and be sure to remain incredibly careful with where you store that information and who you allow to have access to that data.

By considering your data to be important currency, just as you do with your real-life money, you will be well on your way to keeping it safer than most tend to do.