What's next

Authentication & Fraud Prevention, Customer Engagement, Enterprise

# What I Talk About When I Talk About Security

Sometimes the best questions are the ones that don't get asked often enough. For some, not knowing what to ask is half the problem. From a CISO's perspective learn how you and your families can be safer and more secure online by avoiding digital trails of information to reduce vulnerability and risk.

**Leslie Nielsen**

Posted October 28, 2020

When people find out what I do for a living, there is usually one of three reactions, they walk away, they say something along the lines of “*you must never have trouble finding a job*“, or, they ask questions about security, I wish more people would ask.

Many of those conversations fit into two buckets, online privacy, and online security. Essentially, they are one and the same. The more an attacker knows about you and yours (privacy) the easier it is for them to exploit you (security).

The simplest example is almost always social media. I try to frame it this way, if you found yourself in a crowded area surrounded by criminals (the Internet) would you loudly announce that you have nice expensive stuff in your home (pictures of yourself and your house you post online) and that you will be away from said home on vacation (vacation pics and status updates).

The astute then ask, rightly so, "*If that was such a big deal then why aren t there multiple stories about those types of break-ins in the news?*". Good question, and the answer is that I was being allegorical.

## Don't post your digital autobiography

Cybercriminals, at least the good ones, don't waste time on people they know little to nothing about, instead, they cast a wide net and attack soft targets which they can easily gather information on.

Take a few minutes to look through your (and your family's) previous social media posts some time, is there information that could be used to impersonate you and gain access to your bank accounts? Look in the backdrops of pictures, look at your post and connections for names or information that you may use for password recovery, the list could obviously go on and on.

Information is key in a targeted cyberattack, you don't have to be a ghost on the internet, but you also don't have to post your digital autobiography constantly.

It is great to have many connections on social media, but use this simple litmus test to cull your network down a bit: if someone is trying to sell you something, they are not a friend, they are a salesperson and you can unfriend them without remorse.

## Good habits and simplicity pay dividends

I lock my car in the garage, not because I think someone is going to break into my garage and steal my car, but because I know that if I always lock my car, then the likelihood of it being left unlocked outside my garage is significantly diminished.

Discipline and good habits are core building blocks for safety and cybersecurity, lock your computer when you are not using it and use good strong passwords that you change on occasion.

Simplicity is also key, make sure that you disable old, unused, and unnecessary accounts, if you aren't watching it, someone else may be. Absolutely make sure that any information that has to do with accessing your online accounts is secure, if you have an old email address as an option to reset your bank account password, then someone can use it to get into your bank account.

## Start with your personal security, and personal information security

It is a complex world and we can’t fix everything and be 100 percent secure, but we should almost always start with personal security and personal information security.

Personal security is specific to you and yours, how many people have keys to your house, does your home alarm cover all the ways a criminal could enter your house, at end of the day, your home should be the hardest to get into when you are in it because your families safety is more important that the safety of your stuff.

When it comes to personal information security, in addition to simplicity and deactivating old accounts, take a prioritized inventory of what is important.

Finances are usually top of the list, how many banking and retirement accounts do you have, do you know how to access all of them, and how to limit access to them? Did you know that generally, you are significantly less liable when you use a credit card versus using a debit card because you can avoid having to enter a PIN whenever possible for a card transaction? Plus, if your PIN is compromised you may not get your money back.

Does a utility provider really need to know your Social Security Number or Federal Tax ID? The less you share the less likely you are to be impacted if they are compromised.

In other words, the less information you share online means more security for you and yours.

## Understand vulnerabilities, threats, and risk

At the end of the day, we are all pretty good risk managers for things we see, an automobile heading towards us, a wet floor we might slip upon. But we are usually not as good at managing risks that we can’t see such as the extensive criminal element on the internet.

Here is a guide for helping you define and manage risks; it is basic cyber security risk management and might even get you through a high-level meeting without too many action items.

- Vulnerabilities: a bug, a missing patch, a misconfiguration, a weak password, the list goes on and on. For the most part, the best way to think about vulnerabilities is that they are ways that you can be exploited
- Threats: often called Threat actors, these are the people that use vulnerabilities to steal your stuff
- Risks: when there is both a Vulnerability and a Threat that can exploit it, you have a Risk

Going back to the home security analogy to explain this simply:

- Your back door doesn’t lock (*the Vulnerability*)

- There is a robber breaking into houses in your neighborhood (*the Threat*)
- You could get robbed (*the Risk*)

In my world of risk management, there are all kinds of additional details we may add such as likelihood, impact, owner, and status. But the most important thing that you need to know is this:

> *The Threats are already out there, you need to determine where you are a Vulnerability so that you will be able to better manage the associated Risk.*

Rule of thumb, if you are spending all your time worried about an asteroid hitting the Earth, you are a bad risk manager.

To sum up I will leave you with this: **the best way to stay safe and protect your family is to reduce your attack surface**.

Those who know me are no doubt tired of hearing about Attack Surface Reduction, but think about that in your everyday life, and do the things that are going to decrease your Vulnerabilities!

Be diligent and stay safe,
Leslie

**Tags:** Cybersecurity Awareness, Risk Management

## About Leslie Nielsen

Leslie Nielsen, Chief Information Security Officer (CISO) at Nuance, is on a mission to keep employees and customers safe and secure. With more than two decades of cybersecurity experience, Leslie has served on many Fortune 500 steering committees, is a member of the Google CISO Advisory Board, and an invited speaker at security industry events. Prior to Nuance, Leslie held multiple executive-level positions including CISO at SAP SuccessFactors, SAP Concur, and the SAP Cloud Business Group. Leslie was a Practice Manager for IBM Security Intelligence & Operations, CTO at SOS Security, a Forsythe Company, and CISO at Premier Farnell.

View all posts by Leslie Nielsen