TECH

The Real *Michael Claytons*

Author: Bryan Cain-Jackson
Published: March 25, 2013 at 4:34 am

Your interest has been peaked. Especially if you're even slightly familiar with the film *Michael Clayton*, you are already aware that Michael was a fixer of things.

It was for that reason that he was always on someone's hit list. Michael's resources were far too vast for his own good.

The gentleman and his team that we speak of today represent us – the common folks. We either punch in a clock thus working for someone else or we employ others. These people we employ rely on our sound judgment to protect them as well as the company they work for.

Anyone reading this could be toggling back and forth between this extremely engaging article and balancing their checkbook via their online banking. Wink.

Did you just know that just from being online, you stand the threat of being hacked? There isn't a single person that accesses the Internet that isn't vulnerable to being compromised.

I know what you're thinking – you've been lucky thus far, if your habits don't change then why would you fall victim now and not before?

If Beyonce Knowles can be hacked, what makes you think you can't be? There are 19 new victims of identity theft every minute of every day. That translates to 10 million people every year – a figure that is seeing rapid growth.

Your place of employment is vulnerable – the place that has your personal information and cuts you your paycheck is no more or less vulnerable to a cyber attack than you are. According to the Huffington Post, nearly two-thirds of U.S. companies reported cyber security or data breaching in 2010.

Steve Lee and Associates is a firm of… Well, he'll describe it best.

"Well, no one blows up my car. Thank goodness!" Steve laughed. "It's funny, I've thought about this before. Someone else did describe us as a firm of *Michael Claytons*. At first, I resisted that. We're more sophisticated with certain things, cleaner with that line of work. You could dress this up and say that we're forensic accounting with claws and x-ray vision. At the end of the day, we are fixers. We fix problems that other people would find to be intractable. Generally, we can quickly, intelligently and as legally fix a situation. *Michael Clayton* crossed the legal line a few times. We have a far more creative utility belt within our means. To sum it up, we're *Michael Clayton*, Inc."

Steve has more than 20 years on the job and has dealt with the physical and online security of dozens of high profile figures in the world of entertainment and business.

When it comes to cyber security, it's a pretty vast territory when it comes to what we should all concern ourselves with.

What are some of the things that you find yourself worrying about most as an Internet user?

Maybe it's being able to say that we feel completely secure when accessing our bank accounts online, our emails, shopping safely, and making sure no one can spy on our activity.

"Let's look at this from the perspective of an organization. How do I protect my stuff? How do I protect my people's stuff? How do I ensure that our stuff doesn't travel outside of the circle of trust? This is a concern for a number of reasons, it's my responsibility as the principal to protect my employees – there's also the matter of it being a fiduciary responsibility with regards to sensitive financial data. There's information that's proprietary, it could be designs or even trade secrets. This is all looking at it through a prophylactic lens."

Everyone has their own version of the circle of trust. Each computer user could have their Norton 360, McAfee or whatever other Internet security software they choose to use and feel that their safety has been ensured. How many people on the consumer front are actually aware of the fact that many threats are not stopped or even detected by their Internet security?

"I hate to sound like Chicken Little. I would be astounded if that figure was 5% had any appreciation for how insecure their information is, or frankly how lucky they've not had to suffer that kind of a loss."

Many Internet security companies guarantee complete protection. The estimated statistic for actual protection is quite alarming – a mere 65%.

"This is an area where corporations and we consumer are alike. At the end of the day, we're checking the boxes. We feel better if we are checking each box that ensures us the security that we're paying for – all the while, we're not actually safe. What does 65% mean? Is it possible to be 65% pregnant? Or 65% alive?"

Protection from threats comes in just as many forms as actual threats themselves. There is almost always a perpetrator behind every threat – most of the time we are never able to identify the individual who has committed the crime.

Then there are those times where we are able to identify them, in fact we suspect it might've been that employee that worked for us that we recently had to let go.

Cyber bullying and cyber stalking have become such frequent events in today's

society that it has now drawn the attention of our nation's leadership.

Cyber bullying often involves a repeated behavior with the possible intent to harm and by nature can also be repetitive. Some examples are repetitive e-mails and text messages that are of a harassing or sexual nature. It is typically perpetrated through harassment and cyber stalking. The perpetrator will often attempt to damage the victim's reputation and friendships by exposing false and cruel rumors. Online impersonation is also a something that is a form of cyber bullying.

Here is a scenario that Steve is going to walk us through that is typical of the types of requests for service that he gets.

A CEO of Fortune 500 company reaches out to Steve after an employee they were just forced to lay off gave pause as he was being escorted out of the office. The CEO was recommended to call Steve because this is his area of expertise. However, the CEO doesn't feel they are in any real danger.

They ask the question:

What's the worst thing that could happen?

"That's a silly question." Steve states. "It's not something I would say to a prospective client. However, there are two silly questions. What's the worst that could happen? Also, what's most likely to happen?"

The situation being what it is today – an economically distressed economy that shows signs of recovery that are mainly reflective of how the top one percent of wealth is living. Someone who has just been let go from their job after 25 years, 5 years from retirement, and to add insult to injury they've been an exemplary employee while their friend who calls in sick every Wednesday has just been allowed to keep their job. This individual felt secure, but fell victim to the system simply because of their salary.

In this type of situation, there is no limit to what can happen after an employee has been laid off in these circumstances. Sometimes people snap.

"Let's approach this in a reasonable and measured type of way. In order to determine what the worst thing that could happen is we're going to have to learn about who this person is. What led to his dismissal? What did he say? What was his role in the organization? There could be a need for concern."

“Does this guy still have access to the systems? What type of access does he have? Have we made sure he’s been locked out or deleted? What type of work did he do? Would give him access to any confidential information about you or anyone you care about? That information could be used adversely.” Steve said.

“So, what we need to do next is get on the Internet and really quickly learn as much as we can about this guy. Is he the quiet type of person that just had a momentary outburst because he was upset about losing his job? Or is someone that spends four or five hours a night blogging about violent things about other people? What’s his background? Who is this guy? What do you do about him? Is he a felon? Does he have a criminal background? Has he had restraining orders taken out against him? Has he engaged in domestic abuse? Substance abuse? All of these questions are going to paint a picture of what type of an individual we’re dealing with here and it will tell us what precautions need to be taken.”

This is referred to as a threat assessment. It’s all about learning what the perspective client’s vulnerabilities are.

It’s already quite apparent as to why hiring a professional is important. In a panicked state, no one would think to ask these questions. It could cause someone to act out abruptly and irrationally. Approaching a potentially dangerous situation from an organized point of view is always a recommended course of action.

“Answering the question; what’s the worst thing that could happen is a pretty broad question. It takes finding out information to answer that question. In the majority cases, we’ll say that we don’t think this guy doesn’t appear to present a threat. However, you can never know for sure. The best thing to do is to be prepared and be organized.”

For more on how you can better protect yourself and be prepared, visit Steve's website.