ThreatAdvice

Cybersecurity Journal

NXTsoft

An Exclusive Interview with Frank Abagnale of *Catch Me If You Can* Fame!

2019 | $5.95

The ABCs of Cybersecurity

The Future of Privacy

And More Inside...

"CATCHING" UP WITH FRANK ABAGNALE

Interviewed by: Steve Hines

CATCHING UP...

A Rare Interview With America's First Social Engineer

Frank Abagnale is ThreatAdvice's current spokesperson. Steve Hines sat down with Frank where he shared interesting facts from his past and his thoughts on today's cyber world.

Catch Me If You Can covers your teenage years. What was your early life like?

I actually grew up just north of New York City in Westchester County in a little town called Bronxville. I was one of four children in the family, the so-called middle child of the four. I was educated by the Christian Brothers of Ireland in a private Catholic school called Iona in New Rochelle, New York, where I went to school from kindergarten to high school.

When I reached 16 years old in the 10th grade, my parents, after 22 years of marriage, decided to get a divorce. Unlike most divorces where the children are usually the first to know, my parents were good about keeping it a secret. I remember being in the 10th grade when the Father walked into the classroom and asked for me to be excused from class. When I came out in the hallway, the Father handed me my books and told me that one of the Brothers would drive me to the county seat where I would meet my parents and they would explain what was going on.

The Brother dropped me at the steps of a stone building. It said Family Court. I was a little young — didn't really know exactly what that meant. When I got to the lobby, I was ushered into the back of an immense courtroom where my parents were

standing before a judge. I couldn't hear what the judge was saying or my parents' response, but eventually, the judge saw me and motioned me to approach the bench. He told me that my parents were getting a divorce and he needed to know which parent I chose to live with.
I started to cry, so I turned and ran out of the courtroom. The judge called for a 10-minute recess, but by the time my parents got outside, I was gone. In real life, my mother never saw me again until I was in my 20s, and my father actually never saw me again, ever. He died in an accident while I was in prison in France which is unlike the movie that had me going back and forth. That didn't actually occur.

After the day you ran out of the court, you never saw your father again?

No. I ended up on the streets of New York City. My father actually owned a stationery store in Manhattan on the corner of 40th and Madison. We all had to work in the store in the summer, so I made deliveries for my dad on a bike. I knew the city very well. I was comfortable in the city. I went to New York City, which was just a 30-minute train ride. But I soon realized I had to find a way to support myself.

I did have a little money in a checking account that my dad had set up for me from working. I started writing checks, and I found it very easy to go in and ask somebody to cash a check for me, and they did. They were $15, $20. But it then started to get more difficult. They started to tell me, "You don't have a bank account here. We can't cash your check for you."

One day I was walking down the street on Fifth Avenue and I saw an airline crew come out of a hotel. I thought to myself, "Boy, if I could get this uniform and I could become a pilot, then I walk in the bank as a pilot, that would give me such credibility." I finagled the uniform. I basically changed my date of birth on my driver's license. At 16, we had a driver's license, but back then they didn't have photos on them. I was actually born in 1948, but I took the four and converted it to a three. That made me 10 years older.

Abagnale was interviewd in the basement of Shipt's headquarters in Birmingham, Ala. in an old bank vault.

I started going into the bank as the pilot and said, "Hey, I'm on a layover here. I ran a little short on cash. Could I cash a check?" Never had a problem. I quickly realized the power of that uniform. They weren't paying attention to me or the check. All they saw was the uniform, and I realized the power of that uniform. Everything I did in that early career was because I was an adolescent. I had no fear of being caught. I had no fear of consequences. I didn't sit out in front of the bank with a $500 check and say, "Here's my plan. I'm going to go in the bank, cash this check. If they say this, I'll do this. If they do this, I'll do that." I just went in and did it. I always believe, to this day, that had I been a little older, 22, 25, I would have never done half the things I did, because I would've rationalized it'll never work, you can't get away with it. But because I was so young, it gave me the confidence to do a lot of the things I did.

But even so, everything led to something else. Then I realized I could fly on the planes for free. I could stay in the hotels for free. Everything I took on, an impersonation of a pilot, a doctor, a lawyer, there was a reason behind it. It was not the desire to be a pilot, a doctor, a lawyer, but a means to get to my end goal.

So after you decided , "Okay, I've got to quit being a pilot because this is catching up to me," what made you decide, "Okay, it's time to do something different," and what did you do next?

It wasn't so much that. I had a lot of money, but I moved to Atlanta, Georgia into a singles complex called The Riverbend Apartments. On the application for the lease, one of the questions was occupation. I didn't want to write airline pilot, because the next question said employed

by, supervisor's name, phone number. I just wrote doctor.

But I had a very inquisitive apartment manager, so she said to me, "Oh, I see you're a doctor. What kind of doctor are you?" I just said, "Oh, I'm a medical doctor but I'm not practicing medicine right now. I left my practice out west to come invest in some real estate I have." "Oh, how interesting. Well, what type of medical doctor are you?" Then I figured being a singles complex, pediatrician would be pretty safe, so I said I was a pediatrician. Then I moved in. Everybody thought I was a pediatrician but I wasn't practicing. But then I met a real pediatrician, so I started reading up just to keep up conversation with him. Then he invited me up to the hospital where he worked. I met nurses and other doctors there. The next thing you know, he comes to me and says one of the doctors had a death in his family and they need somebody to come up for a couple of weeks and supervise a shift. It's just an administrative duty, not operating or treating anybody, and could I cover the shift.
First, I tried to get out of it by saying, "Well, no, I can't do that. I'm not licensed to practice medicine in the State of Georgia, only in California where I had my practice." "Oh, this is an administrative capacity. They just issue a temporary certificate. You don't need to do that." I thought to myself, "Well, let me see if I can get away with this," so I ended up being the doctor.

Then at the hospital, I met a candy striper, which is a little different than what they show in ***Catch Me If You Can***. Her father was the attorney general in Louisiana. Back then, pilots would go on furlough, so they wouldn't work for three or four months, but most of them all had lawyer backgrounds. They're entrepreneurs, because you only work 80 hours a month when you fly. It was very common to say, "No, I fly for Delta, but I've been furloughed for six months so I'm doing this till my furlough's over or they call me back."

So I say to this candy striper, "I went to law school, but I didn't practice law because I went to fly planes, and I'm on a furlough." And she replies, "Oh, you know, my dad's looking for attorneys. You should come to Louisiana and meet him." I went down and met her dad. He said, "Absolutely, I'd love to have you on the staff. Of course, you have to take the bar." Basically, I took the bar several times, and each time I memorized a lot of what I was taking or got wrong, and finally passed and then practiced law.

I was always smart enough to know that whatever I did, you could only do it for a period of time, but sooner or later they'd catch you. You had to shift gears and change to something else or eventually people would catch on.

So you used your personality and charm as a means to get people to maybe overlook some things they might not normally. Do you think that was, in a way, a method of what we think of today as social engineering?

Absolutely, and that's why there are many writers who refer to me as “The Father of Social Engineering.” Of course, I never realized that's what it was, but here I was, 16, and said, "How do I get a pilot's uniform?" I basically placed a phone call to Pan Am's executive headquarters. The switchboard answered. I said, "I'd like to speak to somebody in purchasing." The clerk came on and I said, "Hi. My name's so and so. I'm a co-pilot with the company based out of San Francisco. I have a problem." "What's the problem?" "Well, we flew a trip in here yesterday. I sent my uniform out through the hotel to have it dry cleaned. Now the hotel and the cleaner say they can't find it. I have a flight in about six hours. I need to get a uniform." "Well, you know, you have to pay for the price of a uniform." "No, I know. I'll be happy to pay, but I didn't know what to do." "Well, you go down to the Well-Built Uniform Company on Fifth Avenue. They're our supplier. I'll call them and tell them you're coming and they'll take care of you." That's exactly what I did.

Again, never realizing it was social engineering ... but the more I did it, the more I realized, "You can get a lot of information from people just by talking to them on the phone." Keep in mind, this is way before computers and the internet and the things you could do today which make social engineering so much easier than when I did it.

Back then, to change your identity, you basically altered your driver's license or you had to make up some phony identification. Today, it is so much simpler to do. Because of the internet, you can change into hundreds of different identities. There was a lot more work involved in doing it back then. It always amazes me that you would assume what I did 50 years ago would be more difficult today, when actually, it's 4,000 times easier today than when I did it.

Let's take a perfect example. When I

started actually really printing checks, I needed a Heidelberg printing press. It was a million-dollar press back then. It was 60 feet long. It was 18 feet high. It required three operators. I spent eight months learning how to operate this press. There were color separations, negatives, plates, typesetting and chemicals to make plates. Today, basically, you sit down at a laptop, open it up and ask for a diagram of a check and a very sophisticated blank check appears on your screen. Then you look out the window and you see Delta Airlines' logo, so you go to their website, capture their corporate logo, put it up in the left-hand corner of the check. You pick a nice picture such as a jet taking off in the background of a Delta tail, and you put it in the background. Step and repeat and in 15 minutes you've created a beautiful four-color check on your screen.

Because we live in a too-much-information world today, all I have to do is call my victim. I call Delta Airlines, get the switchboard, say, "Yeah, I'd like to speak to someone in accounts receivables." Clerk comes on. "Hey, I was getting ready to pay a bill, but we would prefer to wire you this money. I need wiring instructions." "Oh, yeah, we bank at SunTrust Bank in Atlanta, account number 176853." Any bank, any company you call today and tell them you're wiring them money, they have to tell you all the instructions that you would put on a check, routing number, account number, bank name.

You go to the bank's logo on the website, capture their logo, put SunTrust on there, put in the MICR line, and then you call back to Delta, ask to speak to someone in corporate communications. They come on the phone. You say, "Hey, I was getting interested in investing, and I would like to get a copy of your annual report." They mail it to you. Page three is a signature of the chairman of the board, the CEO, the CFO, the treasurer and the controller. White glossy paper, black ink, camera-ready art. You scan it. You digitize it. You put it on the check. It's amazing how technology has made these things so simple!

You've been working for the FBI for 43 years now, trying to help them catch people that do things like you used to do. What made you make that turn?

If I didn't tell you this, I'd be conning you or lying to you. People love me to say, "Well, you know, you were in prison, religion turned your life around, you found God, you were born again, you decided that prison rehabilitated you and now you're a good person." None of that happened. Being the opportunist I was, the FBI came to me, gave me an opportunity to get out of prison.

I just saw that as, "Well, this is a way to get out of prison. I'd much rather be out of prison." I took it, never dreaming about, "I'm going straight. I'll never do this again. I'll never break the law again." But then two things happened. First of all, I met my wife on an undercover assignment. I fell in love with her. She knew me as a totally different person. I even met her family as a totally different person. One day, I had to leave that assignment I was on and I broke protocol to tell her who I really was and how much I cared about her. She married me against the wishes of her parents and we've been married for 43 years with three wonderful sons.
She trusted me. She believed in me. She had faith in me. I didn't have a dime to my name. I was a ward of the government. Basically, she turned my life around. Then when you bring a child into the world, fatherhood changes your life completely. You realize the tremendous responsibility you have for another human being. All of that was a big part of changing my life.

Secondly, when you surround yourself with 12,000 FBI agents who are truly the most ethical people, have tremendous character, love of country, love of family, that starts to rub off on you - their character, their ethics, their right and wrong. I think the combination of both of those things are what really changed my life.

Let's talk about where we are today - how do you see cyber criminals and their ability to get away with crimes versus back in those days?

The big difference today is there are no con men anymore, because you will never see your victim, and your victim will never see you. In the old days, a con man, which stood for confidence man, was a person who dressed very well, spoke very well, had a lot of charm, and he was able to convince people to do things they probably wouldn't normally do. Today all that's gone. The person you're speaking to on the phone or through that email is sitting in Russia in their pajamas with a cup of coffee in their kitchen.

They don't really have a lot of emotion involved. Even in the old days, even a bad con man would eventually say, "Okay, I'm not going to take all this guy's money because I don't want to leave the guy desolate." Because he has a face.
There was a little emotion involved.
Now, these people never see you. They couldn't care less. You're just someone on the other end, a voice on the other end of a phone or an email. That's where it has changed a lot. There is no emotion. It's very ruthless. They're just out to get whatever they can get from you, and that's a big part of what all these scams amount to.

The number of criminals has increased exponentially because it's so easy to do today. I used to teach in the FBI class about the Nigerian scam 20 years ago.
It was by letters. They mailed them out. Someone would raise their hand and say, "Well, look, if they sent out 10,000 letters, who's buying all these stamps?" I would explain to them, "No, the stamps are counterfeit." They're just sending letters out hoping that of the 10,000 letters they mailed, one-tenth of 1% will respond. Today, I can send out 10 million emails, and again I'm back to one-tenth of 1% to respond. Technology has just made this so much easier, certainly made it global. We

used to deal only with criminals within the confines of our own country. Now we deal with criminals all over the world. Even if I know who you are, and I know what apartment you're in in Moscow, I don't have the ability to go arrest you, and I'm not going to get cooperation from the authorities in Moscow to arrest you. The person in Moscow feels pretty safe that nothing's going to happen to him.

What does the term "crime as a service" mean to you?

Crime on the darknet has become so commoditized that you can go on there and even if you don't have a technical acumen or capability, you can contract with somebody who does. They'll help you launch attacks and then you share the proceeds. Again, how easy to sit in a room and do something like that, versus going out, printing checks, going out, cashing the checks, the risk involved of cashing the checks. Today, you're able to get on and sell data and information, whether it starts out at $3 a piece or $10 a piece, or $1,000 for a set, and make a lot of money. Credit card information, et cetera.

Again, most is done globally so when they're doing it, the chances of someone catching them and coming to arrest them are very slim. Today, we prosecute like one in every 700 identity theft criminals. The FBI does not even investigate financial crimes under $100,000. If they do investigate it over $100,000, it's up to the U.S. Attorney to prosecute. Most U.S. Attorneys have a benchmark of $250,000. A lot of criminals know, "If I stay under these thresholds, the chances of me getting caught, one, two, prosecuted, three, getting jail time for it is pretty slim." The risks have gone way down. The rewards have gone way up. It's become a lot easier to do.

So the chances of being prosecuted for these crimes today are much less than forty years ago?

Right. Look at the fact that I was a teenager who did this, so I went to prison in France. I served time in Swedish prisons. I was extradited back to the U.S. and a federal judge said I was a youthful offender because I had committed all the crimes on U.S. soil before I was 21, but still gave me 12 years in federal prison. I served four of those 12 years before I was ever released from that prison. Then we read today that people get out after three months, six months, three years in prison. It's just absurd that not only is it easier to do, but there's very little risk.

If I told you, "Look, you can make $4 million but you'll have to spend 12 months in prison," you'd say, "Absolutely. Show me how to do it." There's really no deterrent, is what I'm basically saying.

We read about and hear about on the news the different cyber breaches daily. What is the profile of a typical cybercriminal? I know you being involved with the FBI probably deal a lot with China, North Korea, and different places like that. Who's committing all these crimes?

Many times, it's state-sponsored, or the state in the case of, say, Russia is turning their head the other way knowing that those criminals are committing the crimes, as long as they get information for them as well. They know it's going on, but they're not doing anything about it. The same could be said about China.

Then there are individuals who do this. As you know, I've always said that it's not really hackers who cause breaches. It's people. What happens is people don't do the right thing, or they fail to do the right thing, or they make mistakes and they're only human beings. They're the weakest link.

Perfect example, I live in South Carolina. Four years ago, someone hacked into the tax revenue office and stole 3.8 million tax returns of the citizens of South Carolina. That was everyone, including me. If you had paid your state taxes by check, they had an image of your check, so they knew where you banked, what your account number was, what check number you

were on, how you actually signed your check. If you paid by credit card or debit card, they had that information.

When that breach occurred, I got a call. I was in the FBI office in Phoenix, and I got a call from our local TV station because they knew I had been a victim, and they wanted a comment from me, knowing how much I've dealt with identity theft. I said to him, "Well, let me ask you this. What does the tax revenue office say?" "Oh, they said they did absolutely nothing wrong." I said, "That would be absolutely literally impossible. Somebody did something."

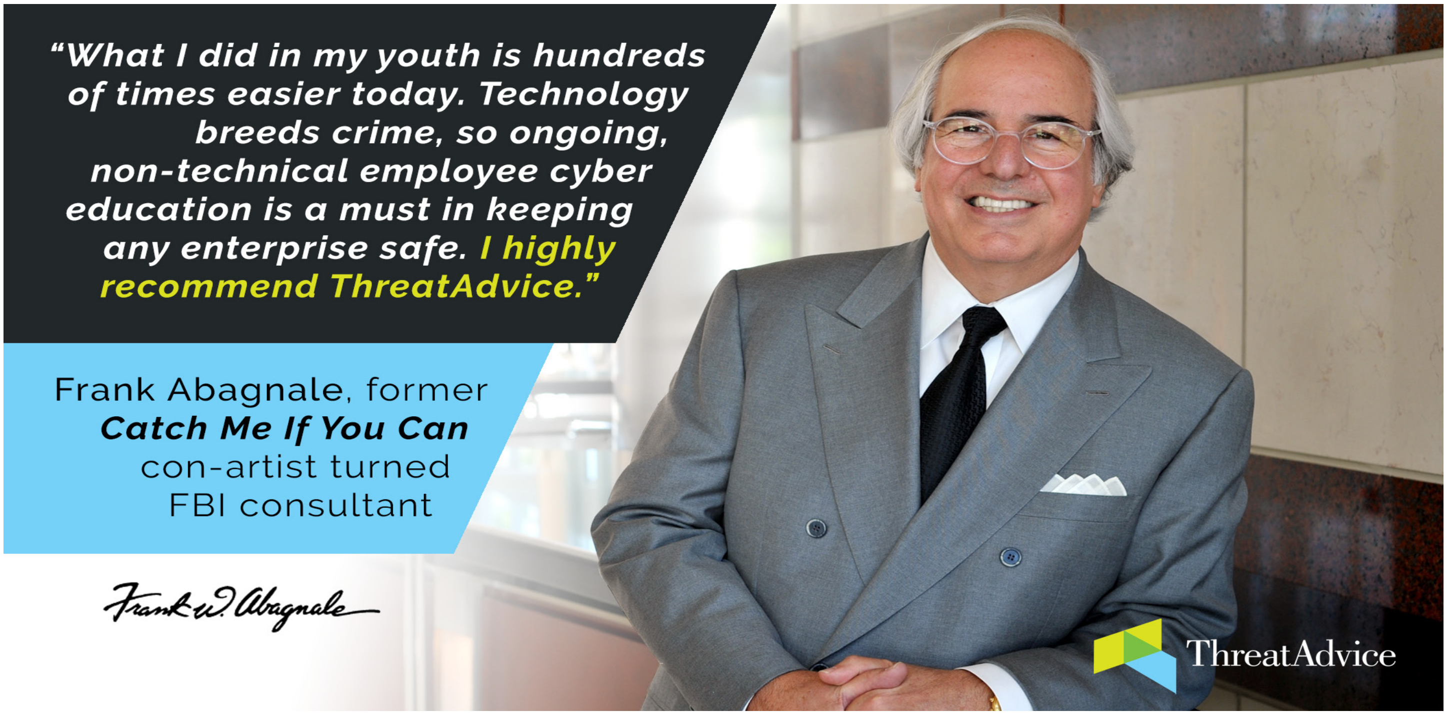
After a two-month Secret Service investigation, it was determined an employee took home a laptop they weren't supposed to, opened it in an unsecured environment. The hacker got in. Our then governor, Nikki Haley, former ambassador to the U.N., ordered that everyone be paid a credit monitoring service for one year. I didn't know the governor, but I sent her an email from D.C. and told her this would be a waste of money and the taxpayers' time. People who steal mass data warehouse that data, usually for three to four years. If you steal credit cards and debit card numbers, you have to get rid of them almost immediately. They have a very short shelf life. But if I steal your name, your Social Security number, your date of birth, you can't change your name. You can't change your Social Security number. You can't change your date of birth. The longer I hold it, when I go to sell it, the more valuable it becomes.

First, you've already told them I got one year of credit monitoring service so they're monitoring my credit, so I'm not going to do anything for at least one year. That's why these breaches, there's a long period of time between the actual breach, and then people start to feel comfortable and say, "Well, nothing ever came of that," and then all of a sudden they start having issues. So much time has gone by they don't even relate it to that. "Well, that must have been from that Target breach a few years ago." They don't even think about that. They think it's something they did wrong - that they gave somebody information they shouldn't have given them.

The weakest link in that South Carolina situation was the employee who took home the laptop or mobile device and was on an unsecured network or whatever the situation was, and that ended up ... I can't even imagine what the cost, total cost, would be to the state. If they did the credit monitoring, that's a fortune. The notification would be a fortune. There are probably some legal issues that come up, and so really, in that case, I think it sounds like a perfect example of the weakest link being a person being lazy or uninformed one time, clicking on one thing, and it ended up costing millions of dollars.

The South Carolina tax commissioner contacted me and said, "How much can we pay you to come in and educate our employees about how important it is to keep this information safe?" I said, "No, you don't need to pay me. I'm a citizen of this state. I want to make sure my neighbors' and my information is safe." I made maybe six visits to our tax revenue office in Columbia. I worked with helping educate those employees.

But the employee in question who took the laptop home, no one ever told her, "This is what someone can do if you get in this uncontrolled environment and they get this information. They can get into the system. They can steal all this data." You have to educate people in their job, to explain to them, "You have an extremely


"What I did in my youth is hundreds of times easier today. Technology breeds crime, so ongoing, non-technical employee cyber education is a must in keeping any enterprise safe. I highly recommend ThreatAdvice."
Frank Abagnale, former Catch Me If You Can con-artist turned FBI consultant
Frank W. Abagnale
ThreatAdvice

important job, and your number one job is to keep the information entrusted to the company by its clients, its customers, its citizens safe. That's your number one job." You have to teach them about phone calls that are using information to get information from you, and soliciting information, emails and how to read emails.

This is what impressed me so much when I first heard about ThreatAdvice. I literally said, "I don't know of any company that does this." I get asked all the time, "Well, where can we get this training?" I don't know anybody that does that kind of training, that's so badly needed, whether it be a bank, a corporation, a government, a mom and pop store.

To have somebody basically teach, in a very simple, easy to understand, not make it difficult and involved, that this is why it's important to keep information safe, this is how you keep it safe, this is when you know someone's trying to gain access to information, whether it be on the phone, on the computer. Again, that must be taught, just like seniors need to be taught what calls are fallacious and phony and what emails are phony. They have to be taught that. They're not going to just know that.

What are your thoughts about social media?

As you know, I've written three books on identity theft. I started writing about identity theft back in the '80s before anyone ever heard of identity theft. Basically, I always remind people if I go to Facebook, I only need two pieces of information about you. All the rest is kind of irrelevant to me. But if you told me on your Facebook page where you were born and your date of birth, that's 98% of me stealing your identity. That's all I need to know.

Now, if you were foolish enough to put a photo of yourself such as a graduation photo, driver's license photo, passport-style photo, then facial recognition can be used to take that photo and put it somewhere else, use it for identification, or literally snap a photo of you in the airport and through facial recognition like Find a Face and many other technologies that are out there, like PitPat. I'm able to basically track you down simply because your picture's on Facebook by using facial recognition. We complain a lot about people stealing our identities, but in the same token we keep telling people more and more about ourselves and then wonder why they stole our identity.

Tell me your thoughts on the cost and impact of a breach to an organization that is compromised.

There are so many things you can do. For example, if I breach a law firm, and I have all the data on all their clients, their clients' children, and their clients' grandchildren, and then I say to them, "Unless you pay me this amount of money, I'm going to release all of this data," there's a ransom side of it where I can extract money from people. There's a side of it just me taking that information and selling it to somebody else who will disperse it and use it against somebody. All of that is due to the cause of failure of you. You caused that breach to occur. That information got out there.

It's very important that companies, corporations, banks realize that you have to prevent crime. You can't rely on the government, the bank to protect you, or the police. You have to think ahead, and you have to be smart enough to make sure that you are educating your employees to deal with these issues every day. You can't just set it aside, saying, "Oh, that won't happen to me," or, "We never had a problem like that."

People bring that up to me all the time, and I say, "Well, let me ask you this. Do you have life insurance?" "Yeah." "Do you plan to die tomorrow?" "No." "But you have life insurance, right? You have home insurance?" "Yeah." "Your house going to burn down?" "Oh, no, I hope not." "But you have it." It's the same way here. It's insurance against having that happen to you and happening to your clients, which you should be protecting your clients.
There's a quote on my website from 1976 where I simply said that the restitution and the recovery of funds is so rare that the only solution is prevention. That's the same thing, today.

Prevention would be there's some software that can help you, but you would say the most important piece is just making sure your back doors, i.e. your employees and vendors and other ways, have enough knowledge to be able to not do or click on something they shouldn't and let the bad guys in.

What I like about ThreatAdvice is that it is educating people. It's not me saying, "Here's the best software, put this in and it'll catch most of these things you have to worry about," so your employees can be stupid about it because this software will catch everything, which is not going to happen.

ThreatAdvice teaches employees in a very simple, again, easy to understand, not difficult format, so once they grasp that, they're able to deal with these issues as they come along. But if employees never have that training, they would never even understand they're being socially engineered or scammed.

Being breached can cost a company billions of dollars. Now I speak at a lot of insurance companies that are introducing cyber insurance. But when I go speak to them, I say to them, "I would not write this insurance unless you can assure me, as the policyholder, that you have educated all of your employees on how to deal with these problems, that you have systems in place to protect the company from having these problems." It is amazing to me that you'd want to go write insurance and not do that, because then if you have a loss, and it was the cause of an employee, that's because you didn't train your

employee. Then the insurance company's taking a huge hit.

It would seem to me it would behoove the insurance company to say, "Look, I'll cover this, and the fact that you do these things have to be in place or my policy is null and void." This is the same thing I've said to insurance companies 20 years ago when they were writing errors and omissions insurance, forgery insurance, fraud insurance. I said, "Look, you have to say to the company a bookkeeper can't write, sign, and reconcile. You have to separate those duties. You have to reconcile on a timely basis, every 30 days. If you're not doing this, and six months later you find a fraudulent check for $100,000 because you didn't reconcile, then you don't pay that claim." That needs to be in your policy, and that's the same with cyber today.
I think more and more companies that want to buy cyber insurance to cover these accidents are going to see they're going to have to train their employees anyway because the insurance company is not going insure them unless they can provide documentation that they've done so. If you have that documentation, that's going to go a long way to lowering your premium, or whatever that premium is, from that insurance company.

What about the breach notification law that all states have now? You've got to let your clients and customers and people that are associated with you know, "Hey, your information was stolen because of me."

That is an expensive proposition for sure and many companies don't have a plan for that. Equifax is a good example of that. Then when it happens, they're all sitting there going, "What do we do? Let's not tell anybody. Let's wait 60 days, see if we can figure out what's going on," all of those things that get them in a lot deeper trouble and put them in a much more liable position. Companies need to ask themselves, “What's my plan if we do have a breach? What steps do I need to take?” Again, the most important thing would be, first, let's not have the breach, so let's take the necessary steps to prevent one.
But yes, it costs the company millions and millions of dollars, not to mention reputation, and their trademark, or years they've been in business. They do business based on their brand, and how it destroys their brand from one little incident. Even if you don't put the money side of it, the destroying of the brand eventually destroys the company and the company's image.

What about forensic costs – getting professionals to come in and get a company or organization back up and running after a breach?

That is another substantial cost. That is why, if someone said to me, "Look, you can spend X amount of money, educate your employees," and here's another thing. If you say to me, "Here's Bank A, they have a great program in place where they educate all of their employees about making their bank cyber safe," that is a tremendous value add to me as a consumer or a business person than Bank B that says, "No, we don't do anything like that. We don't have any programs in place like that."

Obviously, it is also a great value add to say, "We train our employees." A lot of times, people like to keep those things secret, like, "Well, you know, we really educate our employees about that. We have great programs in place. We test them constantly." They don't want to tell anybody that, and I say, "No, tell them because that's what sets you aside from everybody else." That's a tremendous value to me.

Have you seen, on the legal side, litigation relative to easy class certification? Have you see a proliferation of attorneys that are kind of going after these companies that have been breached?

Absolutely, and we're seeing more and more laws where the government is basically regulating and saying that you will be held liable if that breach was caused by a mistake you made or something you didn't do that you were supposed to have done. Equifax has hundreds of lawsuits against them that they'll eventually have to settle or pay out of court that could have easily been prevented.

It's very important to always look at

prevention. What can I do to make sure I'm not a victim? It's just like your house. How do I make sure I don't have a fire? Do I have smoke detectors? Do I have a fire extinguisher handy, that I don't keep things in my garage? It's the same thing in a business. What can I do to make sure I never have this problem?

One of them, and the most important of all, is to train your employees because they're the first line of defense, but they're also the weakest link, so that's the most time ... you want to spend your money and your time.

What do you see today as the top two or three targets, if there are a top two or three, for bad guys as a whole?

My personal opinion is I think in the next two or three years, you're going to see a breach of millions upon millions of search engines, so that I can say to the mayor, "Hey, I know this is what you look at on your computer, and I'm going to tell the world that unless you pay me this." Think of all the things people look at, whether it's medical, whether it's pornography, whatever it is, what they say on their computer, their emails, all that. I think we're going to see where it's not a half a billion, it's going to be a billion or more breaches of search engines.

Now I might not get money out of the average person if I say, "I know you're looking at pornography on your computer." But if I'm the president of a bank, the mayor of a city, a politician, a chief of police, those would be prime targets who have a lot to lose if their reputation is compromised.

Do you, from an industry standpoint, find that one industry or two industries above all is the most lucrative for cyber criminals today?

If you ask me, “Who should be ThreatAdvice’s main customer?” without question it would be a financial institution. Any company handling somebody's money and keeping their information safe should be using ThreatAdvice. All companies absolutely should, but number one is the financial industry followed by the health industry.

Where do you see the whole cyberwar, going from now to five or 10 years from now?

I've always said that at a point, cyber is going to turn dark. As of now, cyber is all about making money and stealing data, which data is money. But if I can get the ability to shut your pacemaker off, if I can take control of your car, if I can get into your bank accounts and things of that nature, or even control some of the health issues you may have, that's where it becomes dark.

I can shut off an electrical grid. I can shut off a bank. I can shut off a lot of things. That's going to become more of a terrorist tool, more of a state tool to make the other country less effective. I think that's where cyber is going. Up until now, it's all been about money and finance, but it is slowly becoming a very dark tool to commit a lot of worse crimes.

I also think what ThreatAdvice provides is going to become not something you'd like to do or maybe you'd consider doing, it's going to become mandatory, because the government's going to get into more regulation of keeping this data safe, just as they've done in Europe. They're going to start mandating that if you have a company, you have to educate your employees about keeping that information safe, and you're going to have to be able to document that and say, "I've done that."

Again, let's say that you have done that. Think how far that goes if you were sued to say, "Well, I've done everything I can possibly do. I've put in the best systems. I've trained my employees. They can testify that they've gone through these programs." That's just a positive for you. That's why I'm so excited about working with ThreatAdvice, because I truly believe that is the key to helping cut down a lot of these cyber risks now and in the future.