



OVC
Webinar Transcript
Identity Theft and Cyber Crimes
February 19, 2013

While Waiting to Begin...

Announcer: Ladies and gentlemen, thank you for standing by. Welcome to the Maryland Crime Victims' Resource Center *Identity Theft and Cyber Crimes* Webinar. During the presentation, all participants will be in the listen-only mode. Afterwards, we will conduct a question and answer session. If you would like to ask a question during the presentation, please use the chat feature located in the lower-left corner of your screen. If you need to reach an operator at any time, please press *0. As a reminder, this conference is being recorded, Tuesday, February 19, 2013. I would now like to turn the conference over to Mr. Russell Butler, Executive Director of Maryland Crime Victims' Resource Center. Please go ahead.

Identity Theft and Cyber Crimes

Russell Butler: Good afternoon, everybody. This is Russell Butler from the Maryland Crime Victims' Resource Center, and on behalf of the National Identity Theft Victim Assistance Network, we would like to welcome you to the Webinar of the crossover on *Identity Theft and Cyber Crimes*.

Check the Box That Best Describes Your Background

Russell Butler: We are going to start with a poll. So, if you would, in the check box, please indicate the best response that describes your background.

Russell Butler: All right. So here we have the poll. It looks like we have a lot of victim service providers, and a lot of others. Well, thank you for joining us today. Let me tell you a little bit about the National Identity Theft Victims Assistance Network. With funding from the Department of Justice Office for Victims of Crime, Maryland Crime Victims' Resource Center, [unclear] created the National Identity Theft Victims Assistance Network. There are 10 coalitions in nine states, and the project seeks to help the field's capacity to respond to victims of identity theft.

Find Out More About Our Network!

Russell Butler: If you are interested in finding out more about the Network, you have the website of the National Network and information about the 10 coalitions on your screen.

Presenters: Michael Kaiser, Executive Director, NCSA

Russell Butler: So, at this point, it is my honor to introduce Michael Kaiser. Michael is the Executive Director of the National Cyber Security Alliance (NCSA). He served as Executive Director of the National Cyber Security Alliance since 2008. Michael engages industry, government, and nonprofit leaders in far-reaching efforts, including Stop, Think, Connect campaign, National Cyber Security Awareness Month, Data Privacy Day, and the National Cyber Security Education Council. Michael has 25 years in all of nonprofit operations, including program management, administration, and governance. Prior to NCSA, he served the field of victim service, holding senior staff positions at the National Center for Victims of Crime, and Safe Horizons in New York City. And with that, I am going to turn it over to Michael Kaiser.

Michael Kaiser: Thank you, Russell. Let me just say it is an honor and a privilege to be speaking to you all today. Russell, I really appreciate all of the work that you have done personally, as well

as Maryland Crime Victims' Resource Center. I think you all are a tremendous resource for the field, and really trying to do a lot of fantastic work in all areas of victimization, but especially today, since we are talking about identity theft—in the area of identity theft. So I really appreciate the opportunity to speak today. And let us have at it, and let us talk about some of the issues in cyber.

Learning Objectives

Michael Kaiser: We do have some learning objectives for today. Hopefully, you can see these on your screen now. I am not going to go through them in depth, but we are going to try and cover a lot of issues. We are not going to go in extreme depth in many areas, so please use that question box to ask questions when we get to that part of the presentation a little later on in the afternoon. I would be happy to try and answer specific questions. I know often on presentations like this, people come to listen, but often have one burning question that they would like to get answered. And we will try to answer as many of those as we can in the second part of the presentation.

Critical Infrastructure: What We Talk About When We Talk About Cyber

Michael Kaiser: So, I want to start by talking about, what do we talk about when we talk about cyber? You know, cyber security is a word that, if you are not in the field, could have—and even if you are in the field, for that matter—can have lots of different definitions. But one of the key areas of cyber that I think sometimes gets overlooked for sort of the more general public point of view, or the “inside baseball” point of view, if you will, is critical infrastructure. And if you have been listening to the newspapers, sorry, listening to the news, reading the newspapers recently, you know, you will hear people like, you know, Secretary Napolitano and Leon Panetta, you know, former Defense Secretary, you know, talking about, you know, a cyber Pearl Harbor. And when they talk about that, they are talking about the potential for an attack on what are called critical infrastructure.

Michael Kaiser: And the slide here shows, I believe there is 18 of them, areas of critical infrastructure. And you can see that they include some things like chemicals, public health, the water supply, you know, food and agriculture, energy. And the fear in cyber security, if we were to suffer a big attack, would be that someone would try to shut down that part of the infrastructure. Now, it is not only about a major attack. Right? In fact, cyber security is often, at least from the perspective of the National Cyber Security Alliance, is often about maintaining and building a safe and trusted Internet. And that is part of where I think cyber security dovetails a lot with what you all do in victim services, as well as law enforcement, and some of the others that are on the phone. Because if you look in the upper right-hand corner of that slide, you will see banking and finance, which is really where a lot of the identity theft takes place, and where a lot of that identity theft creates a lot of erosion of trust in some of the most, really, robust parts of the Internet at this point.

Michael Kaiser: All of these other pieces of the critical infrastructure, the reason we are concerned, is that they were becoming increasingly connected to the Internet. But in banking and finance, we know that is really where consumers--and in some other areas as well, such as energy and government, and some of these other ones, they do connect to the Internet, but it is really banking and finance which, you know, has a lot of your commercial operations going on, and where data is being collected and data is being stored that would have an impact on consumers and small businesses and the people that you might come in contact with.

Michael Kaiser: But it is very important to understand this holistic picture of cyber, because—and I think this will be pretty straightforward to people—but as you sort of live in the digital world, you will see now that almost everything is now connected to the Internet in an advantageous way to all of us. However, protecting that critical infrastructure is really what we call cyber security.

What We Talk About When We Talk About Cyber

Michael Kaiser: So, when we talk about cyber, we also talk about different groups of users. When we say home users here, we really mean home users of all kinds and all ages. So security from our perspective, the National Cyber Security Alliance, and when we promote things like National Cyber Security Awareness Month, we talk about cyber security as a shared responsibility. And that means everybody is involved and engaged. And home users, the kinds of people who may be coming to you because they have been victims of identity theft, are very much a part of the cyber security landscape.

Michael Kaiser: Excuse me. I am just getting over a cold here so I may have a couple of moments if I have to clear my throat.

Michael Kaiser: And we consider cyber security a shared responsibility. So that means that everyone has to protect their part of the Internet, and everyone has to do their part to secure the networks that they use or operate. And interestingly enough, home users these days are very much a part of the network. I think the last research we conducted, about a year ago, indicated that about 70 percent of all homes in the United States are operating wireless networks. So we have networks operating everywhere, and at the end of the day, when we talk about cyber security, we talk about only being as strong as the weakest link in any network. And so that could be a home user, which opens up a gateway, and we will talk about that a little bit more as time goes on.

Michael Kaiser: Obviously, businesses small and large, are very much engaged in this effort of cyber security as well. We see businesses as the recipients and guardians of large amounts of data, and we need to work with them to make sure that they are protected. And, of course, government is both a repository of information, a provider of information, and the target of cyber attacks as well. It goes back to that critical infrastructure piece. Right? Who of our enemies would not want to try, if we were engaged in some kind of warfare, would not want to try to take down our government? But they might also just be as happy taking down Wall Street or turning off the electric grid or stopping our airline systems from working, or those kinds of things.

Where is Your Data?

Michael Kaiser: So, the question that comes back to, where is your data, or where is data? Right? And so, obviously, we will start from sort of the bottom up here, and talk about some of the basic things. Your home computer is a vast resource of data. And if people start to think about what is on there, I want them to think about it in two ways. So, you have your own personal information, which is very important to protect. Right? You may have—it is coming into tax season, you may have your tax records on there. You may have school records from your children. You may have some business records if you run some kind of home business. You may have all kinds of other information about you, in some kind, way, shape, or form that you have on your home computer.

Michael Kaiser: This data could come in all different kinds of forms. So think about, as well, that data is also things that are contained in pictures. Pictures, you know, a family photo taken out in front of your house with a picture of your car with a license plate and your street number provides

a lot of personal information about you that you may not think of right off the top of the bat, when you think of the kind of data that is out there.

Michael Kaiser: Your data may be in company databases. Let me go back to the home computer for one second. You also have enormous amounts of data about other people. Right? People are sending you e-mail, so you have their e-mail address. You have contact lists. You may have other information about people in your family, or your friends, like their birthday and other kinds of things. So in the end, we are all a repository of data in the digital age, and there might be much more that you have about other people as well. And we really believe that everyone has to respect the privacy of others and safeguard the data they have. So it is not just data about yourself, it is data about others.

Michael Kaiser: Obviously, your data is sitting in company databases of all different kinds. Anybody you might have a commercial transaction with, whether you are buying things online, or in other kinds of ways they may have data about you. Obviously, there are data brokers who are collecting information about you and using it. Anybody such as your bank, or where you have an extended relationship in some kind of way is going to have extensive data about you, both financial and otherwise. Your name is going to be in government databases, whether it is your local government, perhaps in the real estate tax database, or other kinds of ways.

Michael Kaiser: Your mobile devices—and not only yours, but the mobile devices of others—are a very rich source of data. Right? You know, if you think of your mobile device for a moment, it probably replicates in many ways the data you have on your home computer, and may very well replicate the data you have on your work computer. Or it may be combined and have both your home and work computer all in one in your mobile device. So really, a very, very data-rich source.

Michael Kaiser: Your ISP obviously has, which is your Internet service provider, has data about you. Marketing firms are collecting data about you in different kinds of ways. And as we look toward the future now, we see other kinds of things happening. Cars, for example, I mean, if you have seen some of the new ads on TV about the kinds of things that cars are doing.

Michael Kaiser: Or you see the ways that people are talking about the Internet in the future. We are going to see things like our refrigerator is connected to the Internet. Any of you who have heard the term “smart grid” know that that is an area now underway in the electrical system to try and connect homes, you know, home and other users of electricity to the Internet to track usage, to provide opportunities for people to control their usage in a little different way, and to provide more proactive ways to manage the electric grid, including, on the electrical company side, a much easier way to chart how much electricity you are using without having to send someone to your house every month to look at your meter and read your meter, which is quite expensive. So, there are many more, and you can think about those.

What Information Do You Need to Protect?

Michael Kaiser: So, when we think about what needs to be protected, there are lots of different things. I think normally when we think about this, we think very quickly of, “Okay, I have got to protect my name, my address, my Social Security number, my birthdate, my children’s names,” all of those kinds of things. And those, obviously, are very, very important elements of your personal information. And each one of those elements of your personal information has a different kind of value. The more someone has about you, the more they can engage in identity theft. Right? And I think that is a theme that we should be thinking about throughout this

presentation today are the different kinds of ways that people might use this data. But obviously, if someone has your name, your address, your Social Security number, and a few other things, they have all of you. And that is a lot of information to have.

Michael Kaiser: Obviously, we talked about this a little earlier, you could have all different kinds of records and statements and things that contain information of a personal nature that could be combined with other kinds of information. So, whatever you are getting, whatever kinds of statements you are getting, you know, statements from your health provider, from your bank, any kinds of tax statements that you are getting. You know, it is tax time, we are all getting, you know, reports back in of any interest we earned from any other kinds of accounts, and those kinds of things, all coming across now. A lot of that either coming electronically, or available electronically, and may be sent to you.

Michael Kaiser: I already talked a little bit about pictures and other identifying information. Your calendar, where you are going to be tomorrow, next week, next month, at the end of the year.

Michael Kaiser: And here is one that I think we really need to think about a lot, and that is your credentials. So, and we are going to talk about this a little bit more when I talk a little more indepth about cyber crime. But your credentials, which in many cases are your password and your logon, is a gateway to your identity in a whole different kind of way. And I think, you know, as we have seen lately, those are credentials that people try to steal. And so you really need to think of those credentials. And you probably all have heard, you know, have a strong password, over and over and over again. Have a unique password for every single account, over and over and over again. It is really important. So I ask you to sort of think for a moment about, you know, what would somebody learn from you if they got your Amazon logon and password? What would people know about you if they had your Facebook logon and password? What would they find out about you if they got your banking logon and password? And for those people who have the same password for all of those accounts, you are basically making it extremely easy for people to develop enormous amounts of intelligence about you in an extremely short period of time.

Michael Kaiser: And then, of course, when we talk about business records, and this is where—and really, it is going to depend on what kind of community you are in—but there are a lot of people that work from home now. There are a lot of people who run small businesses that they run out of their homes, or basically their small business is almost like a home environment, you know, because it is one or two people in a small office, or perhaps a small store, or, you know, some kind of small firm, you know, that is construction or something. And an enormous amount of information can be in those business records. Not only information about themselves, but about their clients and perhaps their employees as well. So you can think about what other information might need to be protected.

Vulnerabilities – How Data is Lost?

Michael Kaiser: So, you know, here is the data. We have been talking about what is out there. How does it get lost? Where does data get lost? So, there are a couple of different ways that are kind of the classic ways. Infection. Right? So maybe you have heard the term malware, or malicious software that we call malware. That is software that gets put onto a machine or a network that is nefarious by its nature, that is put there to do things to harm you. Malware can take all different kinds of form in what it is trying to achieve. And we will talk a little bit about that more in a minute when I talk about sort of the kind of attacks that are out there. But know that those infections are really a major source of data loss, because they can lead to things like the capturing of keystrokes, which would be, for example, the capturing of your password as you

enter it into a website, or your logon as you are entering into a website, or your date of birth as you are logging into a website. Or an e-mail, the exact text of an e-mail that you might be writing that is of a very personal nature.

Michael Kaiser: So infections are the things that we are extremely concerned about. You may have heard of things called dot-nets, which are basically networks of infected computers. These are networks that are operated by cyber criminals and hackers. These networks are used to infect other computers. They are used to use people's computers to generate spam. They are used to steal credentials, used to steal contact lists. So dot-nets are a phrase you may have heard. They are a very important element in the infection ecosystem, because infected machines can be controlled from a different place, from what they call a command and control server, can tell an infected machine what to do. And you would never know that it was doing it, but things have really changed in the last few years. It used to be we would tell people, "If your machine is slow, if you are getting pop-ups, if you are getting all those things, you might be infected." And that is no longer the truth. The bad guys are like, "Why would I want anybody to know I am on this machine? It is much better for me, and I make more money, if no one knows I am on this machine." So the infected machines and the malware is very stealthy right now. And we will talk about how to fight some of these things a little bit later. But I want you to understand the importance of what infection means in the cyber world.

Michael Kaiser: Phishing attacks and social engineering and spear phishing are really one of the core elements, and probably, I mean, you know, when you think of the kind of folks that you all are going to see, probably these three things, phishing, infection, and spear phishing, social engineering, are the three ways that they may be most engaged in trying to protect themselves. Wi-Fi is also obviously a very important part of that. But we will talk about that in a separate element. So phishing, social engineering. Phishing is basically people sending, it could be anything, it could be e-mail, it could be a post on a social network, it could be what they call smishing, which is basically a texting message. It could be vishing, it could even be a voice mail message. Right? Where they send you a message that basically encourages you to click on a link, open a document, which could lead to infection and do other things that might reveal personal information. The phrase, the term of art in the computer world is social engineering. The phrase of art in the world that most of you deal in is fraud. But basically, what they are trying to do is get people to give information.

Michael Kaiser: Here is an example. And you probably have all seen this. Somebody sent an e-mail to someone that says your account, something is wrong with your account, there is an emergency, you need to logon immediately, click on this link and give us your e-mail and password. That is social engineering in the sense that they are trying to get people to do things which they know they should not do, click on links in suspicious e-mails, but they create an environment where it seems like a desperate moment. You know, you need to do this right away. Your Amazon order, there is a problem with your Amazon order, it cannot be shipped. Your package is lost, please logon right away. Those kinds of things. They are kind of a direct mail approach to fraud in the sense that, you know, this is where a lot of spam comes from. People are generating millions and millions and millions of these e-mails hoping for the same kind of return rate that you might get in, you know, direct mail. Right? If you send out 100 million e-mails, and a half of a percent of people respond to it, that is still a heck of a lot of people's personal information that you are gathering. And because the cost of entry is so low to send those e-mails, they can do them over and over and over again. So, that is social engineering and phishing.

Michael Kaiser: Now, spear phishing, which I think is something, for those of you that might be in law enforcement or are working with small businesses, is really an important element of the

vulnerability ecosystem right now. So the bad guys have gotten smarter. They realize that when you send an e-mail that has typos in it, bad language, other kinds of things, that users are getting smarter, and they are saying, “You know, I do not really think that is from my bank. They would not misspell this word, or they would not do that kind of thing.” So, those kinds of attacks have become less productive for them. But spear phishing allows a very targeted attack. And I will give you sort of an understanding of how this works.

Michael Kaiser: So let us say Acme Hardware Company, a distributor of hardware, gets infected. Right? Through somebody on the company went to a bad website, pulled down some malware. That malware looks for a couple of things. It looks for the customer contact list of that company, and perhaps the sales director’s logon to their password information. So, looking for extremely specific things. It gets that through the malware. They create another e-mail that now looks like it comes from a very trusted source, because it is coming from the director of sales to the contacts of that company. Those people are used to getting e-mails from that person. And so now, an e-mail comes out that says, “Acme is holding a sale this month on, you know, bolts, nuts, and washers. You know, click on the attached PDF to see, you know, all the discount prices for the upcoming sale.” Boom. People trust the source, they click on it. That PDF is infected, and now they have got access into all of these other companies at the same time. And they just keep building and building and building.

Michael Kaiser: And one thing you have to remember about all of this, at the end of the day, in the cyber crime ecosystem, data is the coin of the realm. And data gets bought, exchanged, and it is a highly-structured criminal environment. There are people that collect data, there are people that, you know, take that data and, you know, monetize cards. There are people that monetize that data in other ways, so people sell data to experts who monetize that data. So it is a very highly-structured system, but that initial data collection is really the coin of the realm. So I want people to understand that, because if you read the papers and listen to the news, you are going to hear things like spear phishing coming up a lot recently.

Michael Kaiser: Unsecured Wi-Fi is an extremely [sic] area that people just need to pay very close attention to. Unsecured Wi-Fi is any Wi-Fi that does not require any kind of credentials to logon, even though they do require credentials, like at a hotel, could have hundreds of people on it at any one time, and once you are on that network, you know, there is possibilities that people could gain access to your system. In an unsecured, definitely they can. And, you know, maybe sniffing that network or watching the traffic that goes over it. So that is a real vulnerability point. You know, some of those Wi-Fi, like some of those early attacks, like on TJ Maxx, when they stole like hundreds of millions of credit card information, part of that was sniffing through a Wi-Fi network.

Michael Kaiser: Payment systems has also been a huge area of data loss. We have seen that time and time again, credit cards stolen from companies, stolen from small businesses like restaurants and dry cleaners and the like, when their payment systems are not secured, they have not updated them, and that is a loss of a lot of credit card data comes through that kind of system.

Michael Kaiser: Look at lost and stolen. I think, you know, probably almost everybody has heard about, you know, a story about a government agency or a company. There have been a couple recently that, you know, somebody lost a laptop and on it were, you know, 20 million names. Or a laptop gets stolen. You know, we only think of cyber security as being all electronic, but if someone were to break into somebody’s office and steal a laptop, it could be the same thing.

What Are the Threats?

Michael Kaiser: So, where are the threats? Where do they come from? They come from a variety of different places. So, the external threats, in my mind, really break down into three categories. Now some of you, you know, may have some different ones, but these are, I think, the three major ones that I think we should pay attention to right now. And they all have different goals.

Michael Kaiser: I am going to start at the bottom and say nation states. Right? So nation states, if anybody read *The New York Times* today, you will see there was a huge article about China and their Chinese, and the Chinese military and their espionage organization to try and siphon off information from the United States. So, nation states have a couple of different goals. Right? A) They want intelligence, so they want to steal stuff about what we are trying to do. Right? They want to get our secrets. 2) In the case of—and this is a little more murky, but this is part of a great concern in cyber—the stealing of intellectual property and trade secrets, so trade espionage. You know, you can think for a moment about what would happen if a company in the United States spent \$20 million developing a new product, all of the research got stolen, and then someone in another country could now replicate that project, that product without having to put any money into R & D. It is a huge drain of capital and investment, and a huge risk to our economy. And obviously, nation states at some point may want to go on the offensive and engage in cyber war with us. So they may want to be able to crack our network, stop things, you know, when you look at the critical infrastructure problems, I mean, that is really nation states, and possibly other groups who do not like us. Right? You know, terrorist groups and the like who might want to try and disrupt our economy, disrupt our way of life through a cyber attack.

Michael Kaiser: Cyber criminals are in it for the money, you know? Why do they rob banks? Because that is where the money is. Why are they on the Internet trying to steal people's identities? Because that is where the money is. And those are the organized crime gangs. Most of them are organized. They run anything from a kid down the street, or a local identity theft ring, all the way up to highly organized international crime rings. They are the ones running a lot of the malware, running a lot of the dot-nets, stealing a lot of the consumer information, the payment information, trying to break into small businesses and get credentials for banking and making bank transfers. That has been a big issue lately, they basically create a new payroll and send it off to another country, you know, unauthorized bank transfers. You know, a small business might have \$150,000 or \$200,000 in its account, and they try to vacuum that out. It is a pretty great crime for them because it is very hard to get caught and can be pretty lucrative if it works. And so cyber criminals, you know, are just like other criminals. They are just in it for financial gain.

Michael Kaiser: And hackers are sort of the, you know, they are in the middle. Sometimes they may engage in certain kinds of criminal activity, I mean some of it is criminal by its nature, but they are not necessarily in it for the money. They might be in it more for disruption. They may be in it more for making a political statement of some way, shape, or form. You know, we have seen, you know, like anonymous sometimes, you know, launching an attack against a site they disagree with, or a government they disagree with. Actually, from an interesting—I do not know if any of you have tracked the case in Steubenville, Ohio, but there has been, you know, they have actually gone in and hacked some of the evidence in the sexual assault case there, that has been quite a big stir in the community and revealed some of that on the Net to try and show that there is corruption or other things going on. So they can work in different kinds of ways.

Michael Kaiser: The issue with hackers, and to some degree with cyber criminals as well, is that they are non-aligned. Right? They are not nation states. They are not necessarily aligned with an organization. Sometimes they can just be groups of like-minded individuals who could be

operating across the globe. This is a, from my perspective, one of the most interesting emerging areas, because if you think in the past, you know, in order to create an attack on another country or even another group, you needed physical locality and you probably needed the backing of some kind of organized, you know, organization. But hackers can work in the wild, and align themselves either individually on their own or align themselves with a few other like-minded folks. It is a very interesting dynamic that we have to face.

Michael Kaiser: Then, of course, you have the internal threats in cyber, which are unhappy employees who may decide to, you know, steal data and sell it. Bad security practices, which we will talk about a little bit in a little bit more, some of the things you can do to address that. And then you have things, you know, like accidents. You know? Data accidentally get lost, got left in a car and somebody stole the laptop. Or somebody had some stuff on a thumb drive and left it on an airplane. All kinds of things like that, and then just straight-out theft. You know, somebody breaks in, steals your computers, does those kinds of things, or, you know, steals something out of a hotel room. And those are some of the threats.

The Data Loss Environment

Michael Kaiser: You know, I think a lot of you know about this data loss environment at some level. I think some of the things that we are concerned about, and has been in the papers and the news a lot lately, is the number of households with young people who are getting their identity stolen. There is obviously a lot of benefit to the person who steals the identity, for stealing from a young person. If you can get a 10-year-old identity and establish credit in their name, it could be 8 to 10 years of smooth sailing until, you know, anything is found. When that, you know, child maybe graduates high school or maybe graduates college and starts to go out in the world and establish themselves and a credit history, you may have a very long run if you really wanted to engage in that kind of long-term identity theft of a person.

Michael Kaiser: And, you know, we do know that there is a fair number percentage—and I do not know off the top of my head—when I worked in victim services I probably would have been more aware of this number off the top of my head—the number of all crimes that are committed by people that know each other. But identity theft is no different. And we know that, you know, here we see 27 percent, you know, knowing the individual responsible for the crime. And there are reasons for that too. Right? If we think about this, and this is true in other types of crime, like domestic violence and stalking, the more you know about someone to start out with, the more likely you are to be able to steal their information. So if you used to date someone, you are going to probably know a lot about them, you know, you may even know enough to crack their passcode, their password. Right? You certainly know their e-mail, which could be half of their logon. You might know their birthday, if they are using that as a password, or other kinds of things. You may already know their Social Security number, maybe they left it lying around the house. So, you are going to have other information. You are going to have a head start on some of these other folks.

Michael Kaiser: And the corporate side, there is a great report, and you can see here. There is a link to it at the bottom, the *Verizon Data Breach Investigations Report*. For those of you in law enforcement, for those of you really interested in this issue, this is a must-see report. You can... This is the 2012 report, which actually, the 2013 probably comes out in a couple of months. This report is compiled by Verizon, with the help of the Secret Service. And for those of you who do not know, the Secret Service is actively engaged in addressing financial crime. And, you know, this is just some of the record, some of the data that they have: 855 incidents, 174 million compromised records in 2012. Ninety percent of some of the breaches, from their perspective,

were avoidable through simple or intermediate controls, and that could have been anything from, you know, having good antivirus all the way up to, you know, who gets permissions on the network and beyond. Interestingly enough, in the data breach in this environment, you know, 98 percent of it was external. Right? So a lot of times, the internal threat gets a lot of focus. And there are internal threats, do not get me wrong. But in this case, there was a lot of external. And I think, most distressingly, these attacks are not highly difficult. Right? So, unfortunately, in cyber it does not always take a Ph.D. in computer science to launch an attack, especially in the cyber crime world, where you can actually buy what are known as things like exploit kits. You can buy these things. You can buy phishing, what they call phishing kits on the black market, you know, which is basically software ready to go to launch an attack.

Small Businesses an Area of Concern

Michael Kaiser: So, an area of concern for us is small businesses, because they sit on enormous amounts of data and they are extremely vulnerable. When we look at small businesses, well, when we look at the business environment in general here. Right? So the bigger enterprises, the banks, the Internet service providers, your large multi-national companies, the large e-commerce sites, they have been under attack for years. And they have been fighting off attacks for years, and, frankly, they are getting pretty good at it. Not to say that they do not occasionally miss something. But some of you may have heard the phrase, “advanced persistent threat,” or APT. This is something that, basically, people who work in security or the chief security folks, or the security folks in any of these big institutions, they spend their whole days fighting off attacks. They are getting hundreds, if not thousands, of attacks on their networks a day, and they are fending off virtually all of them at this point. Not that there are not other risks, like some of those employee risks, and some of the accidents, and they can lose data in other ways. But they are very defended networks at this point. Small businesses, on the other hand, are much more likely to not have all the security places, security practices in place.

Michael Kaiser: Excuse me again, my little cold here. I did not plan to have a cold when we started this—the idea for this Webinar.

Michael Kaiser: They, they do not have as much need to have in place, yet we see that there is an increasing need for a safe and trusted Internet to be critical to their business. Forty-six percent of the businesses we surveyed last year said that it is very critical that they have that. Yet, the sad news is that 87 percent of the small businesses that we surveyed do not even have a formal written Internet security policy. I think only 70 percent do not even have an informal Internet security policy, which I would define as like, “Hey, do you know you should not be going to that, you know, that website during the day at the office?” Right? So it is a very serious, in the small businesses, and guess who knows that? The cyber criminals know that. And that is why remember when I was talking earlier about phishing attacks and spear phishing attacks? The reason that there are so many spear phishing attacks right now in small businesses is because the cyber criminals know that it is a much more target-rich environment. And if they cannot get in the front door of the big company. Right? By trying to break through the network, maybe they can get in the back door through one of the vendors that they deal with at a small business, or they can just accumulate data on a lot of small businesses.

Mitigate Data Breaches

Michael Kaiser: So, how do we mitigate these data breaches? Well, cyber criminals and others are going to knock on every door until they find an open one. So you have to make sure that all of the doors are closed. And it starts by some pretty simple things, like assessing your risk. Right?

What are your risks? Do you have...Are all your servers connected to the Internet? Do your employees travel? Do they bring their own devices into work? You know, what kind of e-mail is coming over the transom? Those kinds of things.

Michael Kaiser: Monitoring the threats that are out there. Are you aware of the environment, the threat environment that is happening? Are you reporting attacks that are happening to you to places that you might report them? Whether it is...There are some places like the FTC (Federal Trade Commission) and the Internet Crimes Complaint Center (IC3), where you can attack, where you can report some of these things, including your local police.

Michael Kaiser: Do you have a cyber security plan in place? So, there is really two kinds of plans you have got to have if you are going to run—and by the way, I think when I say small business, I really actually include nonprofit organizations. I have been in nonprofits my whole life. We are small businesses. Right? We have payrolls, we have employees, we have, in fact I would say in some of the victim services organizations, we are entrusted with, you know, enormous amounts of personal information about people, about their histories, about what has happened to them. We may actually have vast amounts of information about them. So, a security plan needs to have two elements. Right? It needs to have a strategy going forward, you know, as you build your organization or business. How are you going to keep it more secure? Train your employees. You know, when you add new systems on, when you buy new software, when you source things, you know. How are you going to, you know, maintain a secure environment?

Michael Kaiser: And equally important, what are you going to do if you have a problem? What are you going to do if you have an attack? What are you going to do if data gets lost? How are you going to protect your customers? How are you going to talk to your customers if you lose their data? These are really, you know, how you start to mitigate the potential for data breaches.

Michael Kaiser: Training your employees, very critical here. Even, you know, and it does not have to be super technical either, it can be very simple. Like things about, you know, e-mail hygiene, about machine hygiene. Things around using things like USB memory sticks, which happens to be a huge area of the way that systems get compromised. Right? But also, thinking about, you know, do, are your employees allowed to access their, you know, e-mail from home or the network from home? That has been a source of a lot of attacks, you know, in small businesses. So training your employees and having a plan, thinking about security, thinking about cyber security, understanding that.

Michael Kaiser: We did some research a few years ago, and one of the reasons that small businesses gave that they did not engage in security as much as they should is that they did not think they were going to be a victim. Well, I think we have all heard that from a lot of different people in different kinds of ways, and we know that that is not true. And we know that small businesses are actually a prime target at this point.

Tips for Home Users

Michael Kaiser: So, thinking about all of this, thinking about how we protect people, here are some tips for home users. First of all, you know, if you should—we will talk a little bit more about this in a second too—but obviously collecting and keeping any evidence that you have of any kind of attack that takes places is very important. We like to say—one of our phrases here—we run a thing called the Stop, Think, Connect campaign. The Stop, Think, Connect campaign is a national campaign to help keep people stay safe and secure online. It was founded by NCSA and the Anti-Phishing Working Group. It was created by 25 companies and seven federal

agencies. It is being deployed, the Department of Homeland Security is the lead in the federal government on education awareness on cyber security. They promulgate that campaign through everything they do. Companies like Facebook and Google and Microsoft and ADP and others, Verizon, AT&T, all use the campaign. And one of our major pieces of advice in that is a very simple one. It is keep a clean machine, free from infections and malware. This is the number one thing that people can do to protect themselves.

Michael Kaiser: You know, when we think about cyber crime, hackers, and nation states, when we think about what people can do, we need to get them focused not on the threat, you know, that the, you know, XYZ government is going to try and come and take down their community, because most people are not engaged in protecting against that. You know, that is what government does, that is what their local government does, and that is what industry does that are fighting these threats. But it starts with what they do at home, and how they keep a clean machine. And that really means, it is very simple, it means up-to-date software. And not just security software like [inaudible] and spyware, but the key software that they are using. So whether it is the operating system. Right? That they have, making sure that the patches that come out are installed, whether it is the other key software, like, you know, readers, Adobe readers, PDFs, those things being installed and up-to-date. Or, and also, their Web browser. Very, very important. Web browsers are a vector of attack, and in vulnerabilities, Web browsers is one of the ways that people get attacked all the time. When those updates become available, you must install them and you must do it right away.

Michael Kaiser: Maybe you have heard the phrase, “zero day vulnerability.” That is a vulnerability in the system that has yet to be discovered and been patched, and that is what the bad guys are looking for. They are looking for zero days, so that no one has figured out how to patch it yet, or even knows that the problem is there. And they use those to launch their attack.

Michael Kaiser: You know, when in doubt, throw it out. I mean, this is really just the core advice for everybody on the Internet. Links in e-mails, tweets, posts, ads, that is the way to compromise your computer. Right? Act now, you know, think, you know, do something right away. Be wary of those communications that implore you to act immediately, offer something that is too good to be true really need to be avoided. You know, you just won an iPad? I doubt it. Here is a, you know, here is a certificate for a free Southwest Airlines flight. Not likely. Right? [laughter] So people have to have their suspicious antenna up all the time. I think we know one of the things that the criminals take advantage of on the Internet is that it is a fast-paced, fast-moving environment. And like, ooh, look at this thing somebody just sent me. And when somebody gets hacked. Right? So if somebody’s Facebook or Twitter account were to get hacked and they were to start sending. Those messages look like they come from that person. Right? And so, you know, ooh, you know, Janie is telling me that I got this thing for free now that I did not have before. You just really have to be suspicious, you know. And in a case like that, guess what? You know Janie and you know her personally, you can e-mail her offline and you can pick up the phone and call her. Right? And you can ask, “Did you send me this? Is this really true?” That is one way to protect it.

Michael Kaiser: Owning your online presence is something that we consider to be extremely important. See, some of these are technological, and some of these are educational, and consumer-based action. Owning your online presence is very, very important. What you put online, and what you share online, in many regards is up to you. And so you need to own that. You need to make sure that, for example, on any online service that you are using, any social network or other account that offers security settings or privacy settings, you should always understand how those work, and you should set them to your comfort level of sharing. Some of us

are very public people, and we may want to share a lot. We need to understand the consequences of sharing and the potential harms that could come with that, but if you do that and that is the kind of person you are, okay. And some of us are very private, and we should know how to use the Internet in a way that we can lower our profile.

Michael Kaiser: Secure your accounts, ask for protections. I will talk about this in a second, toward the end.

Michael Kaiser: That password issue again, please, please, please – unique account, unique password, separate passwords for every account really, you know, closes the window on a lot of—well, makes it harder for cyber criminals. Right? So you understand how this works on some level. There are password cracking programs that criminals use, that can go through every single word in the entire dictionary in a short period of time. So, if you are just using a word, or if you are using that awful ‘password1234’ or ‘password’ or, you know, ‘I love you’ or your birthday, it is really a problem. We like to say, long, strong and unique. That is the way to do passwords.

Michael Kaiser: There are a lot of different devices for creating a safe password. You know, some of the ones that we often tell people, the classic ones are use upper case/lower case, use numbers and symbols all combined. In fact, the biggest hurdle to safe passwords is that people are afraid they are going to forget them, which, of course, is true, because we all do. [laughter] So come up with a device. Some people like things like take the first line of your favorite songs, or songs that you like, and take the first letter from each one of those words, you know, make them upper and lower case. Right? Those are easy to remember. Add a, you know, a number and a symbol at the end, or a number and symbol in the beginning or the middle, and that is going to be a much more secure password. So, really, you know, take some time. That is probably the fastest thing. Everybody can do it tomorrow, or when they hang up the phone, you can change your password and make it longer, stronger, and switch them out for different things, and that would be a big help.

Michael Kaiser: And then Wi-Fi. You know, really extreme caution on Wi-Fi is all I can say. Note that your cell phone, when it is connected to the Internet via your cellular carrier, is more secure than a Wi-Fi connection. It is very important to note. Wi-Fis at home should all be, you know, locked down with passwords, and if you are in a public, you know, hotel or those kinds of things, I would just use extreme caution. I would not be logging onto things like my bank or my e-mail or other things. It is fine to go surf for the nearest restaurant, that kind of stuff, but, you know, I would be careful in other ways.

What Victims of Cyber Crime Should be Urged To Do

Michael Kaiser: So, you know, this is about victims of cyber crime. And so, what should victims of cyber crime be urged to do? These are some...This, actually, advice we got really from the Maryland Crime Victims’ Resource Center, and a lot of their classic advice, and I think many of you may know some of this.

Michael Kaiser: A fraud alert, you know, with the major credit groups is really important. So that if in case somebody tries to open up a new line of credit, that you will be notified.

Michael Kaiser: Credit reports, obviously, are going to show you indicators of whether someone has been accessing your credit, or your credit is changing and you do not know about it.

Michael Kaiser: You need to document and keep evidence of all of the things you do, especially when you are, you know, reporting things. But I think if you have gotten, you know, e-mails or things that you think are suspicious, you can save those. It is important...It is important to actually report those as well. You know, you might...Many of the services that you use, your ISP, you might have a spam reporting, or some of the major, a lot of the major e-commerce sites have, you know, an e-mail that you can just forward, you know, like a spoof or a spam e-mail to. You might think, "Well, why should I do that? They have already seen that." But, you know, there is a lot of intelligence in an e-mail. There is a lot of information about where it was routed, where it came from, what the source was and those kinds of things. And also threats tend to come up and down, and it is really important that they have got that data.

Michael Kaiser: Creating an identity theft report, you can do that at www.ftc.gov. I will say that they have an online complaint, as does the Internet Crimes Complaint Center. I think it is www.ic3.gov or .org. We can clarify that. And that is important too, you know, we do not have an enormous amount of information on identity theft. It is not a crime that is heavily reported, or certainly not as reported as it probably takes place. So it is helpful for people to know what is going on.

Michael Kaiser: File a police report, when you can. I think that is really important that we understand, again, you know, crime stats are one of the ways that we focus attention on issues of concern when it comes to crime. So when people report crime, we learn more about how much is happening and maybe get other resources or ways of addressing it.

Michael Kaiser: Change passwords and PINs on breached accounts. Frankly, if you think you lost your data, or if you think in some way that your data was lost, or you get notified that your data was lost, I would go in and change as many of your passwords and PINs as you can, not just on breached accounts, but on all of your accounts.

Michael Kaiser: And back to some of the research we do. So, we do research every October for National Cyber Security Awareness Month, and last year we asked how many people, what percentage, no, we asked people whether in the last year they had been notified by a company or an entity that their data had been lost, and 25 percent of the people we surveyed said they had been notified of such. So, if you are notified, it does not always mean that your data is going to be used or monetized. So, you know, when somebody steals 100 million credit card numbers, the likelihood that they are actually going to be able to monetize all of those, it is pretty difficult. They may sell it to other people, but whether cyber criminals will ever get to actually use your credit card number before it gets canceled by the credit card company when they realize it has been stolen, you know, is a different issue. But anyway, you should change all of those passwords and all of those things.

Michael Kaiser: Now, this next one is a little more complicated, ask for or implement multi-factor authentications where available. So remember, at the very beginning I talked a little bit about, you know, most people just have a password and a logon. Right? So that is how you authenticate yourself. When you put in your password and your login to your bank account, you are authenticating to the bank, I am Michael Kaiser, because I have given you these two identifying pieces of information. Well, multi-factor authentication is when there is a third, or a fourth, or a fifth, or a sixth piece of information that you give someone in order to authenticate yourself. There are many places where there may be multi-factor authentication, which is what we call it in the term of art, where it is available. So, and one of those places, for all you Gmail users, they have one called two-step verification. So you can sign up for that program, and when you logon, they will also sometimes, in certain circumstances, e-mail you or text you to your mobile phone

another code that you have to put in before you can logon to your Gmail. Facebook uses social authentication in a few different places to authenticate. Your bank, some of you may have banks that say, you know, “Give us a picture and then when, you know, you go to logon for certain things, we will show you, and you have to pick the picture that you gave us. Right? Before we will let you into your account.” Some banks may offer key fobs which have revolving, which basically have these one-time use passcodes. So you login with your name, your password, and then you have to look at the key fob and you have to put in a number, and that password is one use only. And 30 seconds after you put it in, it can never be used again. You can still stay on and do everything you need to do during that session, but that number can never be used again.

Michael Kaiser: So these are things that really thwart a lot of the cyber criminals. So I would ask your bank. I would look at the services that you use. They are not always publicly, you know, they do not always advertise it. There is some tension in the cyber security world between security and convenience. Right? Some people think, “Oh, if you have to ask people to put in a second or third factor of authentication, they are not going to want to use my service anymore.” And there are some people now starting to say, you know, maybe having a second or third factor actually makes people trust us more. That is where I hope we go.

Michael Kaiser: And there are some issues, there is some stuff going on in the federal government now around authentication and schemes of authentication that will probably become widely available to the public over the next couple of years. Some of you who really keep close track of this may have seen that there are some people now saying the password is dead, and hopefully we will not have passwords in the future. And that will help a lot, and I agree with that.

Michael Kaiser: If you think you have been attacked, go ahead, alert your financial institution for fraudulent activity. You know, obviously, if you lose any government-issued identification or, you know, even not only government, but I would also say, you know, if you lose the identification for your work as well, please report that immediately. And if you are a victim of identity theft, you know, make sure the debt collectors understand that, and have all of the police reports and other documents that you need ready to go.

Questions?

Michael Kaiser: So I think we are getting ready to talk about questions in a second, so we will figure it out. I see that there are a lot of them coming in, so we will have to address some of those. Just a couple of other resources before we move on to questions. Stopthinkconnect.org, you have heard me talk about that. That is this campaign. Anybody can join it. There is free resources there, you can sign up for it, you can use those resources if you are building a campaign in your community, with all the universal tips and advice, it is all there for you guys, posters, you know, Web banners, tip sheets, a lot of stuff. So come take a look at that. Stay Safe Online, also, our website has a lot of good tips and advice. You can follow us at www.facebook.com, at stopthinkconnect.org, and at twitter.com, at StopThnk, without an “i”, Connect, because somebody had that. And there is my e-mail address, so there is my personal information right out there for all the world to see. I guess we are ready to take some questions.

Contact Information and Q & A

Moderator: Michael, yes, we have had a whole lot of questions.

Michael Kaiser: Okay.

Moderator: One of them was: Can you suggest some additional readings, texts, for people who want to get more information or possibly even teach a course in cyber crime law?

Michael Kaiser: Cyber crime law, I am not as—the law part of it I am not as expert in. I know, Russell, that you wrote a chapter in a book on victimology and cyber crime. Maybe you can mention that at the end of this and encourage people to do that. I think sources of information in this are varied. There are some books, you know, people have written books about, you know, certainly cyber warfare and other kinds of things. People have written some books about identity protection. But this is an ever-evolving threatscape, and I really encourage people to go to things like the *Verizon Data Breach Report*, which will give you sort of the up-to-date information that might be out there, to look for the research. Groups like the Anti-Phishing Working Group which published a quarterly report of their analysis of what is going on in the phishing world and the cyber crime underworld, when it comes to the kind of attacks that are going on. There are a couple of other companies like Symantec and McAfee and some others that actually put out yearly cyber crime reports, where they analyze all of the data that they have. So I am not an expert on all of the books that are out there from an academic perspective, but it is an ever-changing landscape, and I think it is very important to tap into.

Michael Kaiser: One thing that may be of interest for folks that—in fact, a lot of the research in cyber crime actually occurs in the private sector, because they are operating the networks and they are operating, you know, the infrastructure, and they are aware of what is going on across the globe. So I would definitely look at some of those things.

Moderator: I had a couple of questions about Wi-Fi access. Is there any extra precaution that a person should use before using a Wi-Fi, and is there any way to make Wi-Fi safer?

Michael Kaiser: Well, yes. So there are a couple of things here. Depending on what kind of computer you are using, we do not try to get too deep into the technical advice, but usually there is a way. Computers can, on networks, be public or private, and usually there is a way to set up your computer when you logon. Sometimes you might get requested every time you logon to a new wireless network. In other operating systems, you may have to go in there and do it before you go on, that can make your computer private. So make sure it is not public, make sure it is not broadcasting or accessible to other people on the network. Sometimes it has to be accessible, especially in a work setting. Right? Where you might be sharing data and other kinds of things. So it just may be that that is the appropriate mode. On the other hand, make sure when you are on Wi-Fi, or out in the wild so to speak, that that mode is not available.

Michael Kaiser: Back to sort of those basic precautions, you know, the more open the network, the more dangerous it is. Be extremely aware of how you are connecting to the Internet. I mean, if you are down at, you know, Joe's Café and it is like, we have got free Wi-Fi, I mean you have no idea who else is on that network. You have no idea, you know, who is sitting in Joe's back room on that network. I mean, frankly, using those networks at all has some risk, and I would try to stay away from them. On the other hand, if you are on a network that requires credentials, it is always better.

Moderator: So, on a similar vein, there are a couple of questions about people who know that their machine or their network is infected, and they want to know how to get that clean and not become re-victimized. What would you tell those folks?

Michael Kaiser: So, if you think in any way, shape, or form that you have been infected, you need to—well, first thing would be to make sure that your security software program is up-to-date. If

you do not have a security program, better get one right away. Then, I would go to, if you go to actually the Stopthinkconnect.org website and look for, we have a campaign called Keep A Clean Machine, you will find a list of companies that will scan your computer for you, and clean up your computer if there is a problem, for free. They are all free. All reputable companies who will do this. So that is something you can do. So if you think, "Ooh, I might be infected, maybe my security software did not pick it up," you can go to one of these, you know, and you can scan it, and they will tell you if there is a problem. So, you try to clean the machine. If you really are nervous about it, I mean, frankly, you could disconnect from the Internet right away, run your scan on your computer with your local AV program just to make sure, and then, you know, reconnect and then try and go do these things. But, you know, if you really think there is a problem, you should, you know, work on your computer offline for a while.

Moderator: We have a question from someone who works with persons who are elderly, and so they want some suggestions about the elderly and also, because sometimes those people with the elderly have other people who have access to their passwords. You know, any suggestions you have for those sorts of situations?

Michael Kaiser: Yes, those are, you know, and I think...So, a couple of different suggestions. I mean, this is true of families in general. Right? Not just the elderly when it comes to passwords. I mean, how many children know the passwords to their parents' phones. Right? Because these devices are no longer singular devices attached to individual people, they become devices that belong to the entire family, you know, whether it is a tablet or a laptop or a phone. So, you need to use extreme caution with that, and so with young people obviously, you want to teach them about that and not to share it, not to give to anybody else. I understand this point with elderly people who may have other people who are assisting them, maybe helping them pay bills, maybe helping them do other kinds of things, you know, check on account status, do other kinds of things. You need to use caution. I think that even if somebody else is helping you do these things, you have to go in and look for irregularities, things that, you know, maybe should not have been paid, or maybe payments that were made that should not have been paid. Those kinds of things. And I would change, I would encourage those people to change their passwords on a regular basis. Right? So that, you know, if you had a caregiver and they left, and now you have a new one, you should change your password, so that the old caregiver cannot get back into the computer, you know, remotely with your logon and password. So there has to be some management on that side.

Michael Kaiser: I know it can be difficult, it can be difficult for all of us to remember passwords, so I am not picking on elderly people here. I would also say that they should write those passwords down, even though that is not advice that is always given. But they should write them down on a piece of paper and they should put them somewhere safe in their house. I mean, do not store them on the computer in a Word document or a spreadsheet, because those could be lost. But the likelihood that someone is going to break into your house, get into your sock drawer and steal your password list is much less than someone might steal them off your computer. So you can do those kinds of things. I would also just limit the access that people have, and try to make it as easy as possible, or use as few accounts as possible that you give access to.

Moderator: On the same vein, there have been a couple of questions about some of these electronic password keepers. Do you recommend them, or what should people do before trying to use one of them?

Michael Kaiser: Yes. So, that is a great question. So there are a couple of different elements of this. Right? There is the auto-fill, which is available on a lot of Web browsers, which I really

recommend people do not use. Right? I mean, unless you think no one ever in the history is ever going to get access to your computer, you know, you could use that service. But auto-fill just means, hey, the next person that sits down at my computer and goes to my banking site and automatically it says, “Do you want to use your password that is already in there?” Bing, and they are in. So really, especially people who travel, oh my God, you know, you do not want to—your technology may not even be stolen, you could lose it, and people lose stuff all the time. Right? So it is not always, you know, and somebody just turns on your computer and they are in. So yes, I do not really recommend the auto-fill.

Michael Kaiser: Some of the password managing systems, you know, are okay. You know, they should be from a reputable company. There are some of the security software, you know, the major vendors, like if you are already running one of the major security programs, I think all of them now have some form of identity management service in there. You can certainly feel a little more comfortable with those. You still may not want to put everything in there. There may be a couple that, you know, like a bank, maybe you want to keep your bank out of everything and only you know that. It is not that they know your password, but, so you have to look at how it is being managed, who is managing it. But some of those are fine, but the auto-fill, probably not a good idea.

Moderator: What about reporting to the FBI through www.ic3.gov? Is there any recommendations you would have to encourage folks to report crimes?

Michael Kaiser: Yes. So, I would encourage people to report crimes, and I talked about this a little bit earlier, because we actually do not have good enough reporting. You know, if you report a crime to the IC3, you are not – you are not going to necessarily hear back from them. And it is not going to guarantee you that it is going to be investigated. But there are some things that may happen. So, if your crime, if your incident was already part of a larger incident that they were looking into, and I think those of you who work in this field at some level know that there have been some cases where there are literally thousands upon thousands upon thousands of victims. Right? Or if they are making a case, or trying to uncover a new kind of fraud or thing, it is going to be extremely helpful to them. But it is not like issuing, getting a report, you know, to traditional crime, where somebody reports a crime and you expect your local law enforcement, you know, to follow whatever procedures they have for investigating or following through on that crime. That is not – that is not going to happen. But the information getting to the FBI is really critical, because, you know, when we think about cyber in lots of ways, and this is just one of them, our traditional infrastructures have not grown yet to compensate for them. So, you know, we see that in the area of law sometimes, and I think crime reporting is one of those, where we do not quite have the infrastructure together to really collect as much as we need to know. So, I really encourage people to report, with the understanding of—we always do with people when we are working with victims—that that is not necessarily going to mean that their case is going to be personally handled or resolved.

Moderator: We have a tremendous amount of questions of people who are concerned about their own home security, and I know that you addressed that a little bit. But they, people want to know what is the best that they can do for their home Wi-Fi, or what sort of protocol to follow when things keep changing, and how do they know? If you were to just highlight a couple of bullet points, what would you say the most important things people could do to protect their own home networks?

Michael Kaiser: Their own home networks, number one, that every Wi-Fi router should be password protected. So often they come with a—well, actually I should say the router, the router

producers are getting a little bit better. It used to be that, you know, everyone basically came with, you know, a password set as Administrator or Admin. Right? And a lot of people never change those. And so you could drive around town and you could logon to people's wireless networks because it was Admin, and so you just tried it out and you could do a little, you know, stealing of people's networks. And I think we have seen some of that actually, there has been cases like in child porn, where people have tried to get in other people's networks to protect themselves, so it looks like the information is going through a different network. So that is one.

Michael Kaiser: Two, you get to name your network. Right? Usually when you set up a router, or if you have not, and you set it up a while ago, you can go in and rename it or set a new password. You know, do not put, you know, your address. I can see that sometimes. If you open up your computer and look for wireless networks you will see things that have like people's address or people's names or the Kaiser Family Network, you know, that is broadcasting to the world. So, you know, give it some name or give it a number or just obscure thing that no one could ever attach it to you directly. Those would be like two key pieces of advice.

Michael Kaiser: If you have an older router, you might want to just go to the website of that company, and check it out. It is possible that there is updated software for it, and there may be some security patches in that, so you could do that as well. Those would be the three things I think everybody should, you know, take a close look at for their router, for their wireless networks. And then, of course, you know, you are going to, you know, you may be giving out that password to people. Right? So if you have guests come to your house, they are going to need that password, and, you know, you can decide after those guests leave whether you think it is an appropriate thing to change that password, depending on how the visit went. That was kind of a joke. [laughter]

Moderator: Well, we have another question here about bank fraud, when some of this material has—people have caused harm to others. What should they do for resources to respond to bank fraud?

Michael Kaiser: You mean, if they have been individually defrauded or...I assume?

Moderator: Well, in the beginning you mentioned a lot about one of the big areas was banking and finance, and a lot of theft occurs there. They want to know, when theft occurs, what should they do in terms of if it involved using the personal identifying information to get some money out of the person's bank?

Michael Kaiser: Absolutely, report it to the bank right away. You know, in some cases, there may be some protections. Unfortunately, for small businesses, a lot of those are not protected from losses that get taken during a cyber crime. I think there may be some changes coming in that, and there are some civil cases now around, you know, around responsibility and liability for when transfers get made inappropriately. But a lot of the individual consumer is protected, you should definitely report it. You should report anything that is suspicious. You should report and investigate yourself and report immediately any, you know, things that appear on your – on your bank account that do not look like they should be there, that you cannot remember if you ever made that. I know sometimes it is difficult, because sometimes you do business with a company and then when they actually charge your account, they have kind of a different name. But, you know, that makes it harder for us as consumers, actually. And you should just report it and investigate it as soon as you can. And you have to, unfortunately these days, you kind of have to keep tabs on all of these things. You know? Your bank records every month, or, you know, online

periodically, take a quick look and make sure everything looks the way it is supposed to look, and report it immediately.

Moderator: So, obviously, as consumers, people need to worry about themselves and take the appropriate steps, but where do other people become liable if there is a data breach?

Michael Kaiser: That is a great question. You know, you know, it is going to be different in different places. There is no current federal data breach law. Some states require different kinds of notification and different kinds of actions after data breach, and it varies, you know, like notification or maybe credit, you know reporting, free credit checks for a period of time, or other kinds of things. I do not think the liability question is 100 percent resolved. I mean the good news for most consumers, if it involves a credit card, you know, their liability, their liability is like \$50, and I think in a lot of cases the banks do not even go after that. So the banks almost accept all of the liability on some of those kinds of losses. I think in other areas, it can sometimes be, you know, the business could be held liable, and a lot of businesses do not survive a data breach. I cannot remember the number off the top of my head, but Symantec did a report a couple of years ago, and a high percentage of businesses that offered, that suffered a data breach or a data loss in some way, shape, or form actually went out of business in the next 12 months. So, you know, it is an emerging area at some level.

Moderator: So you mentioned there was no national data breach law, but we have had a couple of questions about what is the future? What legislation, what activity might be coming down the pike that some of the people who are on this call might ought to be aware of?

Michael Kaiser: Well, there has been a lot of discussion about the need for a federal data breach law, and, you know, we do not do a tremendous amount of work in that regard in terms of policy. I think there is actually a lot of interest from everybody in that, because it is one of those areas where, especially—and, you know, we deal a lot with larger companies as opposed to smaller companies, but it will be easier for them, for example, to have one data breach law for the whole country, which they could comply with. Right? You know, in one way. And so I think there has been some discussion of that, and I think that could possibly be a good thing for folks, so that we could create a harmonized and universal expectation of what would happen when there is a data breach. And I think that is one of the issues now is that it is not clear for everybody what happens. And it is not clear when companies even need to tell you that they lost their data. So I think, you know, some of that, clarifying that as kind of a community or society-wide expectation, I think, would be a really good thing. Personally, whether it is legislation or otherwise, I think more transparency when data is lost is in everybody's benefit. And I think we have to move away from a lot of, you know, finger-pointing and blaming. Certainly if there is negligence, there is negligence, and we should address that. But, you know, when you have organized crime trying to steal your data, you know, it is in everybody's best interest that that gets reported, because then everybody can do everything they can to fight it.

Moderator: So, there is also a question about where can people find the breaches that are known? Where do people go to find out where the breaches are listed?

Michael Kaiser: Wow, that is a good question. I am not, in all honesty, I am not 100 percent sure if there is a central breach notification area. I know that the Verizon report is very good. That is historical. I know that there is some reporting, obviously, in the media. You know, so if you have a nice Google alert for data breach or, you know, or hacking, and you will find out a lot of what is going on as those get revealed. I know that there are some other groups, and I cannot remember off the top of my head now which ones, that actually do a little bit more active of this, they

actually comb that stuff. So I would actually use your favorite search engine and just ask for a list of data breaches and you might be able to find something better than what I have given you.

Moderator: You may also be able to go to your home state's Attorney General's Office or other consumer office, and they may have lists in your state there.

Michael Kaiser: Oh, that is excellent, that is excellent advice as well.

Moderator: So, there have been a number of people who have asked for the slide deck, and whether it will be available and whether they can use your hints. So, we will make them available, and there is also one particular one that also wants a link on the NCSA website, so hopefully that could be provided as well?

Michael Kaiser: Yes, you can provide the whole deck, as far as I am concerned, to anybody who wants it. I mean, you know, and all our...And just a little, you know, a little advertisement for ourselves, and actually I see somebody in the comments said that the Privacy Rights Clearinghouse has lists of data breaches, and that is one of the groups that was on the tip of my tongue but I could not remember. So that is great advice. Just a note, everything on NCSA's website is free to use, you can take it, you can use it, you do not have to attribute it to us. We are believers in getting the word out. Come use it. On Stop, Think, Connect we have a lot of pre-made materials that people can take, but if they want to use, sort of integrate their message more deeply—and you can find out about this on the website—you know, there are other things you have to do to use that information. But a lot of it is—it is all free, we do not charge for anything. So, yes, come to staysafeonline.org or stopthinkconnect.org, and come take all of the information you want.

Moderator: All right. We probably have time for one or two. Let me try to find a couple. So here is one concerning electronic medical records.

Michael Kaiser: Yes.

Moderator: They are asking because of facilities reporting breaches, what extra precautions should victims whose medical records have been broken into should they take?

Michael Kaiser: Well, I think, you know, medical records, the thing about medical records that, you know, gives me the most pause is that it is an enormous amount of information about you. Right? I mean, really, you know, just tremendous amounts. I mean, we all know, you know, when we go into a medical facility, you know, the kinds of information we have to give. Everything. Right? Name, rank, serial number, Social Security number, date of birth, parents, mother's maiden name. All of these things that go in, and that is our very, very most private and personal medical information. So I think the things that people need to, you know, do around those things is, 1) they are going to have to have very heightened awareness of whether that information is being used in any other way. So, you know, again, back to the basics, you know, the credit reporting, the other things. I would be changing passwords again, I would be looking at my bank accounts, I would be doing all of those things, because that kind of information can be, you know, the gateway to credential information. Right?

Michael Kaiser: Then I think, you know, they probably need to check and make sure, you know, on their insurance records as well, to make sure that someone is not trying to steal their identity and their medical information in order to steal their medical insurance, which I know can happen in some cases. And so they need to be aware of that, and whether—I do not know all of the rules

and regulations about medical identity theft, but I would assume that if you felt your medical records were stolen, you might want to notify your insurance company at some level.

Moderator: All right, last question. Someone wants to know about how to be involved in the future, and what they should do to, you know, help both victims of crime and to be more aware of cyber security. What should they be looking to do in the future to be involved and help people who have problems in this area?

Michael Kaiser: I think there are a couple of things they should do. We like to encourage everybody to take the time to get educated themselves, and then educate the people around them. So somebody asked about older people earlier, you know, if you are educated about this, then you are going to be more able to educate your grandparents, your older relatives. But get engaged. Get engaged in National Cyber Security Awareness Month every October, get all of the tips and advice. Go down, educate your--educate your customers if you are a business, educate your citizens if you are in government, educate your clients if you are in victim services. Take the time to educate the people in your orbit. We use what we call the Trust Network model of education. We believe that people respond to or act on information to be safer and more secure if that information comes from people that they trust. So our goal is to create harmonized, good advice and let people like all of the folks on the phone here today bring that to the people in their orbit. So there is National Cyber Security Awareness Month. There is Data Privacy Day in January. There is Safer Internet Day in February. [laughter] There is whole host of ways that people can get involved. And we encourage them to do that. So come to our websites, use your website, Russell has great information, and educate people around them.

Stay in the Know!

Moderator: All right. Well, Michael, we really appreciate all the time and effort that you gave today to help educate those that are involved in the crossover between identity theft and cyber security. We have your information there online. We will also bring up some information about the National Identity Theft Assistance Network. Just to let people know that we are putting together a toolkit of information that will be available to help people in their community, whether it is an individual organization or a group that wants to form a coalition. And we will be having some replication efforts for those that would be interested in some training and technical assistance in their community. So please feel free to take a look at the resources, and we thank everyone for participating today.

Michael Kaiser: Thank you. It was a pleasure and an honor.

Moderator: All right. Thank you, everybody.

Announcer: Ladies and gentlemen, that does conclude the Webinar for today. We thank you for your participation, and please disconnect your lines.

[End.]