Day Two—Plenary Session V

Background on New Technology Offenses

Scope of Reported Criminal Activity

Jason Thomas, *Manager, National Fraud Complaint Management Center, Internet Fraud Complaint Center, National White Collar Crime Center*

Survey Data on New Technology Offenses by Computer Security Institute

Richard Power, *Editorial Director, Computer Security Institute*

PLENARY SESSION V:
BACKGROUND ON NEW TECHNOLOGY OFFENSES

PROFESSOR O'NEILL: We would like to turn now to a presentation dealing with the scope of the reported criminal activity. This is one of those really interesting areas. It involves the FBI's *National Crime Victimization Survey*—which is I believe, after the census, the largest household survey undertaken by the United States Government—and seeks to get a handle on the number of crimes actually occurring out there; not just reported crimes but, rather, a household survey to look at crimes generally being committed.

It is obviously a much larger number than the number of crimes that are ultimately reported to insurance companies or to the police. The interesting thing about it is that it generally tends to dovetail nicely with the self-reported crimes of criminals in these prison surveys that we have done.

I would like to welcome our speakers to this panel that will be talking about the scope of reported criminal activity.

First, I would like to introduce Mr. Jason Thomas, the manager for one of the National White Collar Crime Center's new initiatives, the Internet Fraud Complaint Center. I would imagine that that is an absolute growth industry; that is what my guess would be.

The system is developed in conjunction with the FBI. He will be announcing a new innovative law enforcement tool and will be using technology to create a nationwide clearinghouse to process fraud-related complaints, support meaningful enhancement efforts in the prosecution of violators, and produce effectual prevention programs to reduce victimization.

I would also like to introduce Mr. Richard Power, the editorial director of the Computer Security Institute. That is a San Francisco, California-based organization which provides a clearinghouse and is really the premiere international association of information-securing practitioners.

Mr. Power is also the author and editor of the annual study, *The CSI/FBI Computer Crime and Security Survey*—a survey, I have to confess, that I am using extensively in an article on cybercrime that I am currently writing. Without any further adieu then, I would like to turn the time over to Mr. Thomas.

MR. THOMAS: Again, my name is Jason Thomas. I work for the National White Collar Crime Center. For those of you that don't know, I want to give you a real quick education on who we are so that you can have an idea of how we fit into the Internet Fraud Complaint Center.

The National White Collar Crime Center is a not-for-profit organization. We are funded through the Department of Justice. Our mission in life is to provide a nationwide support system for the prevention, investigation, and prosecution of economic crime.

To do that, we provide a variety of services to our membership, and our membership is primarily state and local law enforcement agencies. That is our concentration. About two years ago, the FBI approached the National White Collar Crime Center about starting some type of Internet fraud initiative. We got on board and created the Internet Fraud Complaint Center.

The Internet Fraud Complaint Center is set up to receive fraud complaints from consumers, really, around the world, who have been victimized by a fraud occurring over the Internet. We went operational May 8th of this year and, as of September 27th, we received just over 15,000 complaints. That is with little or no advertising.

We did one press release when it opened and have since stayed away from the media as much as we can—and everybody here knows how hard that is. We have also received just over 15 million hits on our website, so less than one percent of the people who are visiting our site are actually filing complaints.

The website is listed there, *www.ifccfbi.gov*. I certainly encourage you to take a look at that and visit that website. Before I get into the stats and kind of give you the scope of the problem—what we do is we take the complaints that a consumer files on line with us, and we refer that complaint back out to the most appropriate law enforcement agency or agencies that have jurisdiction over that complaint.

Obviously, many of the complaints that we get are multi-jurisdictional in nature; therefore, many of the complaints go out to many agencies, state, local and federal law enforcement agencies.

I mentioned that this is a partnership project between the FBI and the National White Collar Crime Center. It serves very well for both organizations. The FBI is, obviously, concerned with federal interest crimes. The National White Collar Crime Center, as a gateway to state and local, can enable those complaints to get out to the most appropriate state and local law enforcement agencies.

So the complaints come in, we store them in a centralized repository, then we forward those complaints back out to the most appropriate agency. Every complaint that comes in gets sent to a state, local, or federal law enforcement agency. Whether it gets worked is up to that agency, but we do get those complaints out.

The complaints, once they come in, can go through a variety of processes. The first process is: we identify a series of patterns that relate to, say, a series of complaints. For example, say we get ten complaints against a specific subject. We see five complaints where money is sent to a specific address, to the same address. We identify those, pull those together. We then go out and gather public record information: web-based information, who owns the website, who sent this e-mail, those types of things. We gather that. We do an analytical summary. We forward that to the most appropriate law enforcement agency as well.

Finally, the last process that these complaints can go through is: once we identify further thresholds and it looks like this thing is really a criminal case, we will also gather commercial public record information from Lexis-Nexis or Choice Points, those types of folks; pull all that together and send that out to the most appropriate law enforcement agency.

So it is a very proactive way of addressing these crime problems. Again, it is up to the law enforcement agency or agencies, if they are going to work it together, to determine how it is going to proceed, if they are going to open an investigation or not.

The stats regarding the complaints that we have received thus far are as of September 27th of this year. Obviously, auction fraud (48%) is a huge, huge problem.

Non-deliverable (19.2%) is not an auction; it is where somebody has contacted me and said, "Hey, I have a $500 computer that I would like to sell you." I send him $500. I don't get any product shipped to me.

Securities fraud (16.9%), credit card fraud (4.8%), identity theft (2.9%), business opportunities (2.5%); and then, professional services—which is bigger than I thought it was going to be, 1.2 percent—and that is where someone is purporting to offer a webpage design service or something along those lines; I pay them for that; they never design my webpage; those types of things. Then we have "other" at 3.7 percent.

These statistics are based on the complaints that we have received that are fraud complaints. We get a lot of complaints that aren't fraud. I would say 25 to 30 percent of the complaints that we get are about child pornography, are about violent crime issues. You would be surprised how many complaints we get from somebody sitting at the computer saying, "I think somebody is casing my house, and they look like they want to burglarize my house; what can I do about it?" So we get things like that. But these stats are based on those complaints that we get that are fraud related.

One interesting anecdote that I would like to relate to you, as it applies to the audience here, and kind of give you an idea of the types of crimes you are going to be seeing coming your way if you are a prosecutor or you are a judge—we recently received a complaint from a former cop who was playing this online game; it is called Ultima Online.

I don't know if anybody has heard of that. It is a graphical game where you can actually own property. And the people who have played it have built up a society, and the property actually has value, real value. The cop who called us or filed a complaint on the Internet said, "I had this piece of property in this game. I sold it to this person. I transferred the deed to them and they never paid me my $500."

She then went on to say that she was driving past the property, looked in, and saw that people were there. I am reading the complaint thinking, "Well, is she really talking about real property, or is she talking about virtual property?" Obviously, she was talking about virtual property. The question is, who gets that? Who is going to investigate that? Who is going to prosecute that?

QUESTIONER: Virtual prosecutor.

MR. THOMAS: Yeah, a virtual prosecutor, exactly. Those types of cases are going to be coming your way very soon. How do we deal with them? I don't know. I don't have an answer for you. I can give you some ideas on how we can start to look at who may be able to work those. But, how we deal with them on a grand scheme, I have no idea. And those are the types of things that we have to be thinking about when we are thinking about future technology offenses.

Some stats on victims, under 20 and over 60; these are normal stats. (See Figure Thomas-1.) This is the kind of thing that you would normally see in a breakdown of victimization, you know, what the age groups are. The highest being 31 to 50; that is where the money is. But, the ones that are under 20 and over 60, I really think you are going to see a huge increase in those percentages.

The reason I think that is because there is a huge push to get our parents online, to get our kids online, to get our grandparents online. It is easier to communicate. It is a great medium. Well, we are putting these folks online without giving them the tools they need in order to reduce their chances of becoming victims. So I really anticipate those numbers to grow or those percentages to increase.

Seventy-three percent male, 27 percent female; that is not really that surprising. The average loss per victim is about $700. So, per complaint, we are looking at about a $700 loss. Pretty surprising stats in terms of what we have seen so far.

Like I mentioned, a lot of the complaints we get aren't fraud related, so we have got those things thrown in as well. The complaints that come in that aren't fraud related—for example, Mr. Vatis mentioned infrastructure protection issues, national security issues—we get a lot of complaints like that. Those that come in that are of that nature or child pornography immediately go out. They aren't even databased within our system; so those things are handled immediately.

So, if you have any questions about the Internet Fraud Complaint Center, I will be more than happy to answer those.

QUESTIONER: You had mentioned that you had 15,000 complaints since September. I was wondering how large your center is, staffwise, and how quickly you can turn those complaints around and forward them on to agencies for investigation?

MR. THOMAS: The complaints we have received thus far have been just over 15,000. The staffing we have, currently, is just under 60 people. It alternates between 58 to 60 people. The turnaround time is not as quick as I would like it to be. When we first opened, we got overwhelmed with the number of complaints that came in. We had no idea that we would get this volume of non-fraud-related complaints. A lot of this is automated. A lot of this we can sort out in the front end, but a lot of this requires an analyst to look at the complaint before it goes out.

Many times, we will have a victim file a complaint and they don't complete the information. We can't classify it internally so we can't tell where it needs to go. So with those types of things we have to contact the victim back and say, "Hey, did you really mean to file this? What is going on? Were you really victimized?" Turnaround time is about a week to ten days to get those out, depending on if we have all the information available.

We have built in artificial intelligence into the system so that we can accurately identify trends within the data. I mentioned that we identify thresholds and things like that, and that is how we do that. That is an automated process.

We will be redesigning our webpage, and we will also be redesigning our complaint form, and that will be out at the end of this month. So, hopefully, we can streamline a lot of the process and reduce our turnaround time from that week to less.

QUESTIONER: Can you tell me or do you have any idea why people would come to you or the Center there, rather than going directly to their local authorities? And, do you encourage that and why?

MR. THOMAS: We don't encourage that. Many of you are aware of how fraud victims react. They are the best investigators that money can buy. Typically, what happens is they go to a local police agency; the local police agency says, "This is what? Internet fraud; oh, I have no idea how to do that. You need to go to the state police." State police says, "What is that? Internet fraud; I don't know how to do that. You need to talk to the FBI."

And that is what happens, and the victim gets tossed around. He gets thrown around. He gets frustrated. They see our website, look to us and say, "Oh, this must be the easiest way to do this," and they send us the complaint.

Now, how do we deal with those issues? How do we deal with those state and local law enforcement agencies and federal law enforcement agencies that don't know how to investigate that? The National White Collar Crime Center—there is more to the National White Collar Crime Center than just this—has a training component that provides training to state, local, and federal law enforcement agencies on these specific types of crimes. Still, there is a huge, huge gap there, but hopefully it is being addressed.

Thank you very much. If you have any questions, I encourage you to give me a call. I want to thank the Sentencing Commission for inviting me. Thank you, again.

MR. POWER: I am very happy to be here. We started our annual survey with the FBI Computer Crime Squad in 1996 because, when they opened their office in San Francisco, they came to me with some excellent questions. I said, "The only problem with these questions is we have the questions; nobody has the answers." So we reached out to the CSI membership, which is information security professionals and Fortune 500 corporations and large government agencies, and started to ask a series of questions, and now we have five years of data.

The survey is free. It is available to anybody. You can request a copy from our website. It has been a pretty interesting process. We start out with a really broad question: have you experienced unauthorized use of your computers within the last 12 months? And you can see that from the five years of the survey, the answer "yes" has grown from around 40 percent to 70 percent. (See Figure Power-1.) I always tell people, you know, there are only two honest answers to this question: "yes" or "don't know." Those organizations that are answering "no," well—anyway.

I guess I have been saying this long enough so that now, if you look at it, "no" has collapsed, and "don't know" has remained pretty steady. Now, "don't know" has gone down quite a bit.

Increase in criminal activity is one dimension of that growth, but another dimension of that growth is that people are looking, and back in 1996, there were many organizations that weren't even looking. By the way, one more thing about this figure, 70 percent, that is taking out computer viruses and taking out laptop theft. That is serious criminal activity, 70 percent.

It occurred to me the other day, the reason we started this is because people were not reporting computer crimes. They were not detecting them. If they detected them, they were not reported. We wanted to encourage people to report computer crime and it reminded me of that old philosophical question, you know, "If a tree falls in the forest and there is nobody there, does it make a sound?"

That 70 percent answers the question, the tree fell. To the question of what part of the forest was it fell in, we asked the question: which point of attack is a frequent point of attack? And you can see internal systems has pretty much remained the same; remote dial-in has actually gone down; with the growth of the Internet, Internet is a frequent point of attack. It has risen to almost about 60 percent. (See Figure Power-2.)

This defies the conventional wisdom about computer crime and computer security breeches—and I have never said this because I don't believe this—that 80 percent of the problem is insiders and 20 percent of the problem is from the outside. That was true in the days of mainframe computing. It is simply not true now. It is not that the insider threat has gone down, but the threat from the outside because of the Internet has increased so greatly.

What types of attack or misuse have you detected in the last 12 months? This is where it starts getting interesting. As I listened to your discussions yesterday, my mind boggled and I said, "Oh, my God, I have really bad news for these people because cyberspace crimes add a whole new dimension of complexity and subtlety to the issues that you are grappling with, and I don't envy you." (See Figure Power-3.)

You can see, if you add in viruses and laptop theft, over 90 percent of the organizations we surveyed have experienced some type of misuse or criminal activity within the last 12 months. "Likely sources of attack" is who felled those trees. Another bit of conventional wisdom—disgruntled employees, you can see around 80 percent; independent hackers, you can see up in the 70 percent area; corporate competitors at 50 percent. No one likes to talk about this in the private sector, but when you give them an anonymous survey to fill out, this is what they are talking about, 50 percent. (See Figure Power-4.)

Last year the Hoover Institution asked me to come and give a talk on estimating the cost of computer crime. I said I wouldn't give that talk, but I would talk on guesstimating the cost of computer crime because that is really what we are still doing at this point, guesstimating. There is no solid methodology to quantify these things. That is why you get very disparate answers and very disparate kinds of data from people. (See Figure Power-5.)

One thing is developing over time and in the survey pretty clearly. Director Vatis pointed out: 270 organizations, $260 million in last year's survey, an average of $1 million per organization. But that is somewhat deceptive because, of that $260 million, $66 million of it was trade secret theft, theft of proprietary information. In fact, it was about 24 incidents of theft of proprietary information. Fifty-five million dollars of that $260 million were incidents of financial fraud; and, again, it was about 20 incidents of financial fraud.

The reason I say this is because when everybody thinks of cybercrime, they think of somebody with a purple mohawk and a skateboard. But this is over $120 million, about 40 organizations, large multi-billion, multi-tens of thousands of employees organizations. This is the real problem. Teenage hackers end up in the headlines because they get caught. The people who are doing this kind of activity are a little harder to get ahold of.

This is a picture of how the losses have been growing over the years. (See Figure Power-6.) We have done the survey for five years, and we have asked the financial loss question for four years. We didn't want to ask it in the first year because we didn't want to scare people off completely.

The growth in the loss figures has less to do with the number of respondents or an increase in activity as it does with the fact that people are getting better at quantifying their financial losses. And you can see that in terms of trade secrets theft in cyberspace because, for instance, in 1997, we had 21 quantified losses for $20 million. In 2000, we had 22 quantified losses for $66 million. Twenty million dollars in '97 and $66 million in 2000, with only one more incident.

Quantifying is also a problem. Most years there are 100 incidents of theft of proprietary information reported in our survey, but only 22 of them are willing or able to quantify them.

People talk about how these things are quantified. How do you get to $80 million? Well, the $80 million is, I believe, where the Sentencing Commission guidelines top off. It was much higher than $80 million. How do they get to a figure like that? The value of a minute of computer time equals total yearly cost, divided by number of minutes in the year, et cetera.. That is one way.

Another way is, for instance, in the case of denial of service attack, a company like Yahoo! does $600,000 an hour in online sales. Anyway, denial of service really interested me in the wake of that attack on Yahoo! and those sites; eBay, the auction site, said they didn't have any losses. Their customers just came back the next day. And I don't know if you know any retailers, but I know brick and mortar retailers, and the most fundamental thing in retailing is you write down on your calendar in the back of your store what you did that day, how much money you made that day, and then you go and look at it the next year to see if you are still making as much as you made the year before.

If you close down a brick and mortar retailer for a day, he would say he lost that much money, what he expected to make that day. So it cracked me up when eBay said they didn't lose anything. The point I am trying to make is that there are serious problems with quantifying financial losses for cybercrimes. Private corporations are having these problems. Government agencies are having these problems. These problems are going to impact your ability to understand how to weigh the severity of offenses.

QUESTIONER: I guess my question is: is there really a loss to the economy and does it matter if, say, eBay closes down for one day and other—maybe brick and mortar merchants—acquire those sales or other e-tailers acquire those sales? Would that truly be a loss to the economy if there is simply a redistribution of sales among the various bookstores?

MR. POWER: That is a very good question. I guess you have to look at it in terms of what the Internet economy means to the country or what it is perceived to mean to the country right now, you know, and to the growth. The economic boom of the '90s, a great deal of it, has to do with the Internet economy. If people lose confidence in that economy in various ways, it could have significant impact.

I think that your point is well taken, though, and that is why I try to talk to people about trade secret theft. You know, there is a case involving Archer Daniels & Midland and the enzyme that gives farm-raised salmon the same pinkish hue as wild salmon; it involved $300 million for this one enzyme. So, when you get into the areas of biotech and high tech, those kinds of criminal activities can have a lot more impact on society.

But, I think the real concern is with situations like Yahoo! and "Melissa" and the "Love Letter" worm; it really has the impact on the Internet economy.

QUESTIONER: I would assert that these numbers are probably underreported. What is your sense of by how much?

MR. POWER: Oh, yes. I am glad you brought that up. They are conservative numbers, and they are the best case scenarios because CSI members—like ISSA members or some of the other folks involved in information security—their having jobs in a corporation indicates that that corporation or government agency has at least some security posture.

So these folks have some level of preparedness, and they are conservative figures, and they are not exaggerating. In fact, in most incidents when you see $60,000 or $100,000 or $200,000, they are really just adding up the cost of the investigation and the clean-up, not the cost in loss of business and other things.

To kind of give a perspective on those numbers—$260 million for 270 organizations in 12 months—I did a survey of hundreds of news stories and, in those hundreds of cybercrime news stories, I found only 11 stories that cited actual financial loss figures. I tallied up those financial loss figures; there was $15 million in a two-year period; $15 million, 11 incidents, a two-year period.

Then, if you add to that the *Mitnick* case, which in court was $260 million—one case, $260 million, involving I think four companies—now we are at $275 million. We have already eclipsed those 270 organizations, so your point is well taken; and that is not even discussing "Melissa" or "Love Letter" worm.

And, by the way, "Melissa" happened before "Love Letter," and "Love Letter" apparently caused more damage, which means that organizations didn't even respond, didn't even learn the lessons of "Melissa." So next time it could be even worse. I agree with you.

PROFESSOR O'NEILL: I would just like to now take a moment and thank both of our panelists for this very interesting presentation on the scope of the cybercrime problem.