SENIOR LEADER PERSPECTIVE: RONALD E. PLESCO, JR.

NSCI's Lindsay Trimble recently interviewed Ronald Plesco, Jr., president and CEO of the National Cyber Forensic Training Alliance Foundation (NCFTA). Plesco is a nationally-renowned Information Security & Privacy Attorney with 14 years of experience in information assurance/privacy, identity management and computer crime law. The NCFTA brings together local, state and federal/international law enforcement and INTEL entities, private sector companies and academic institutions to functionally collaborate and develop intelligence on cyber crime threats and methods.

NSCI: In 1997, you co-founded the National Cyber Forensic Training Alliance Foundation (NCFTA). Can you tell us about the organization and a few of the most significant changes you have seen since 1997?

PLESCO: Sure. The organization today is dedicated towards identifying cyber threats; developing intelligence to mitigate those threats; and, most importantly, to neutralize those threats. That last piece – neutralizing – is key, in that it keeps us one step ahead of the threat. As the threat occurs, you react, mitigate it and then take the threat out and then you can neutralize that threat for a certain period of time. I'm not going to say it's never going to come back; it will, but in different forms. It's better than playing a mitigation game only.

The NCFTA works with the private sector, government and academic institutions to identify what the current threats are, where they're happening, attribution (as to entity, organized crime, non-organized crime), share that intel amongst our private sector partners and assist them in mitigating the threats that are taking place against them. At the same time, we share information with the law enforcement and intelligence community – U.S. and non-U.S. – to assist in the neutralization, or the targeting and arrest of the threat actors that are causing the cyber threats to take place.

Since 1997, the FBI, Software Engineering Institute, West Virginia University and a handful of companies came together to form the NCFTA, more to deal with forensics – not so much network or cyber forensics, if you will. They researched computer forensics to share best practices and information related to that. We found ways to deal with the three issues that I talked about in a proactive fashion, by creating a mutual forum for corporations and various sectors to come in, tell us in a trusted environment – a safe harbor, if you will – what's taking place and how it's taking place. They then permit us to share that information with their competitors and peer firms to better the sector and reduce threats. At the same time, everyone agrees to share that information with law enforcement and the intelligence community so they stay up on the threats and the attribution of the threats.

I'll give you an idea of our partnerships from a high level. In the financial sectors, we have top banks (U.S. and non-U.S.); credit card companies plus the issuers; and brokerage firms. On the non-financial sector side, the pharmaceutical sector is represented; as well as the property rights arena, including hardware and software; the telecommunications sector; and, of course, the government sector.

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **P a g e | 1**

NSCI: It seems "Digital DNA" is key to assigning attribution for cyber actions. Can you tell our readers what "Digital DNA" really is, and how cyber forensics compares to more traditional forensics?

PLESCO: From our standpoint, we look at network flow analysis, IP addresses, network communication and the exploitation of those. At a high level, we examine IP addresses, botnets, botnet networks, what those networks are doing worldwide, what type of clients and the threats that are taking place. Through them, we see the utilization of malware to enable criminal activity to take place.

For us, the two main reasons bad code is written are the following: 1) To take over/own the machine. This is usually unknown to the user or the network to utilize it as part of a botnet or for storage for bad guy networks and organized crime. 2) Credential harvesting from the machine (user name, password, etc.) for e-channel accounts, non-e-channel accounts, as well as credentials for credit card information, payment information and process information.

"Digital DNA" is more of an industry buzzword. We work with very talented researchers worldwide and with corporations that watch what hits their networks to really keep our finger on the pulse of what the threats are and to share that information across our peer groups to meet the three goals I discussed earlier – identification, mitigation and neutralization.

NSCI: What are some things you look for when conducting cyber forensics?

PLESCO: From a high-level standpoint, we look for packet-level analysis as well as IP addresses, proxies that are set up for distribution, establishment or utilization of a botnet network. And we look at content: malware content in a network; the URL itself; applications/executables that are pushed with malware content; and code analysis for that. We look at how – from an operational standpoint – it's being used to commit a crime or a cyber threat.

Then, we synthesize that type of information into actionable intelligence to kick out – not exactly an alert – but an "FYI" to our partners, but more driving toward attribution: Who's doing it? And why are they doing it? Where are they? And most importantly: Why? What does that type of vulnerability that's being exploited by code or through analysis allow somebody to do? For example, were they able to steal money from accounts or set up a dissemination network for child pornography? Another example would be to set up a network for utilization that's part of a spear-phishing campaign. That type of analysis is what we do.

NSCI: How do they help to improve our ability to prosecute cyber criminals?

PLESCO: Identification is the key. Knowledge transfer of what is taking place is a subset of that. Our partnerships are sharing that information. As a former prosecutor, I know that, traditionally, law enforcement has been behind the eight-ball – reactionary to the crimes instead of being proactive. From a law enforcement standpoint, if you can prevent the crime, then there's no need to investigate. If you stay on top of the threat and identify how it's taking place today, you can see what's taking place tomorrow and share information to prevent it. That's a better paradigm than reacting. The key is that

110 Royal Aberdeen ⚫ Smithfield, VA 23430 ⚫ ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **Page | 2**

information sharing regarding the current threats from industry and academia researchers to law enforcement enables law enforcement to stay up on it. This way, they're not just starting anew when something happens and they'll already have a base level of understanding of what is taking place, what has already been done and to what extent it's working. It makes for better background for the investigation when it occurs.

NSCI: With cyber forensics being primarily an intelligence and analysis activity, what improvements do you think are necessary to our traditional intelligence collection, analysis and dissemination processes and tools?

PLESCO: To me, "traditional intelligence" is intelligence-gathering by law enforcement and the intelligence community. Traditional intelligence gathering is all about attribution: Who or what entities are doing X? How are they profiting or reaching their goals? What are their goals?

The tools that exist for that include intelligence databases; data mining; and other tools to gather the intelligence – whether it's human intel, signals intel, network intel, etc. And then there's the analysis of the intelligence. Those tools have always been driven toward the paradigm of nation state/threat actors/organized crime. They've always been really physical and world-based – non-Internet or non-network-based.

What has happened and what is needed are tools that do the analysis from a network standpoint. You need an emergence of the folks that understand networks, such as information security professionals, with the intelligence folks to put together their identification analysis capabilities from an intel standpoint. In my opinion, that needs to take place more.

There are a lot of cutting-edge companies working towards data analysis and visualization of that data. On the network side, an understanding of what is needed for the business/operational side is necessary. A key example is that companies are now working in a proactive way to actively infect virtual machines with the latest pieces of malware identified by the anti-virus companies. Then, they utilize those machines to authenticate their networks or a sandbox – a similar network set-up – so they can watch what effectively takes place when an infected machine comes in. Then they can learn from that and identify, from a proactive standpoint, how to mitigate those threats. From an intel standpoint, that kind of collection activity has not really taken place before. Pieces of it have, but having that effectively take place from private sector companies sharing that information across companies is really key in the immediate, as are the data analysis and visualization folks.

NSCI: Are there any research areas you think need more attention – where our knowledge and/or capabilities simply are not yet up to the challenge?

PLESCO: A lot of companies are pushing the cutting edge of that. There needs to be more research done in the authentication and identification measures for networks. There are some companies that are doing great research and a couple companies that have products to market that have taken advantage of encryption through authentication, down to the chip-level, so each machine has a chip set and the

110 Royal Aberdeen ⬤ Smithfield, VA 23430 ⬤ ph. (757) 871-3578

CyberPro *Improving the Future of Cyberspace...Issues, Ideas, Answers* **P a g e | 3**

ability to encrypt. Some companies are pushing the utilization of that capability, for example from a Windows standpoint, and if you can't do that, at the very least, down to the kernel level.

While there are still threats, you've mitigated the majority of them during this. That type of research needs to continue and companies need to look at those products – from an e-channel standpoint – and be sure they can work with those products and fully utilize those products. On the authentication side, pushing encryption to another level and the organization of that in the e-channels is key; that's one research area.

The other is that the ability to predict analysis of network data flow, from a corporate standpoint, to mitigate the threats based on that analysis. Those are the two that are most important, in my opinion, from a high level. It's happening where it's needed, but I think more cross-sector information sharing is necessary to stay on top of threats and mitigate them.
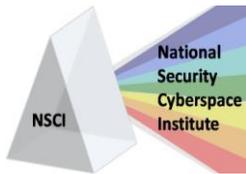
NSCI: How do the skills associated with cyber forensics and intelligence differ from more conventional forensics and intelligence?

PLESCO: It's all technical, but cyber forensics is more network/computer and code-specific. It's more technical, but it's also very different. For example, firearms are firearms; they work in a variety of ways and there is a variety of types, but at the end of the day, they function similarly. In the computer network forensics world, there's a variety of operating systems and a variety of networks that exist. The fundamentals of all the layers must be understood as well as the various hardware, software and applications work. That's what is very different than traditional forensics. You have to identify what is taking place.

For example, the news recently has highlighted the case between China and Google and other U.S. and non-U.S. entities. Traditional law enforcement would respond, investigate and look at the crime scene for evidence. The evidence now is worldwide, it's beyond networks and it's very tactical in nature (understanding the coding and how it's being written). The tools to solve this are out there in the private sector; the traditional law enforcement approach doesn't work. If you look at the FBI, the Secret Service and the U.S. Postal Inspection Service, they're on the cutting edge of keeping their agents up to speed on how to deal with this type of threat. The problem is this type of threat is changing every day and we have to keep our education up-to-date with how the threats play out, as is evidenced by what's happened recently between China and Google.

NSCI: How do the roles of our universities and colleges (e.g. education) differ from more specialized training and/or certification programs?

PLESCO: We work with a handful of universities and, more importantly, we work with students. We hire students as interns – paid and unpaid. The students come from computer science departments and information security programs, but those aren't the only students we bring in. We also bring in law students, intelligence studies students, undergraduate students, etc. The challenge for universities is to extrapolate the education of students on the theory and take from that the practical/business

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **P a g e | 4**

application of the theory. And that's where a lot of universities are falling short. Some are cutting-edge and we're assisting them in those efforts, in that we allow their students to work directly on real-world problems – the problems of the United States.

One of our latest challenges has been since the tragic earthquake that took place in Haiti earlier this year. We're working on what we've termed the "Haitian Earthquake Fraud" and looking at the fraud that's taking place regarding charitable contribution funds. The students understand computer science theory, how networks work, how to communicate, etc ., but that's only part of the puzzle. They now need to take that and apply it to real-world situations, such as the Haitian Earthquake Fraud – where a Web site was established to socially-engineer a rip-off of public funds or utilize those Web sites to distribute malware. It's really the business importance and the practical importance application of the theories.

We're honored to have these students. We're an unusual model; we're a non-profit entity. Those students make us who we are, with their ability to not know a box and to think outside of a box allows us to be successful with our partners and to find and mitigate threats.

NSCI: How important do you think continuing education will be, given the pace of change in cyberspace?

PLESCO: It's huge. There has to be a symbiotic relationship between workers and education. What I mean by that is they have to stay up on those threats. There are a lot of good public relations activities that take place and many networking opportunities that take place at conferences; we've participated in some of those, but that's an old-world model. The new-world model is real-time, to share information 24/7 and to allow them to stay up-to-speed on that. Understanding what type of information is out there and what type of interest exists in your subject matter is important. We offer a lot of that and do that with our partners. That's key.

Continuing education, in the traditional sense, is definitely needed, but I'll take a page from the success of an entity that's two doors down from us – the "Entertainment Technology Center" at Carnegie Mellon University. The professor who started it, and unfortunately passed away last year, Randy Pausch believed that you get your master's through practical experience and through the real-time application of the theories that you learned as an undergraduate student. To me, that's where it's all at.

Unfortunately, I had a master's of information security student who came to me after graduating for some career advice. I asked her what her practical experience was and she didn't have any. I told her she needs practical experience, certifications and accreditations on specific hardware, such as Microsoft or Cisco hardware. There's definitely a need for continuing education.

We've partnered with the University of Pittsburgh, West Virginia University, Carnegie Mellon and a number of universities to give the students an opportunity to apply what they're learning in an internship. I think the world of what Randy started and it's a wonderful model to copy for how education ought to be placed now.

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **P a g e | 5**

NSCI: Numerous cyber-related studies have called for an improved partnership between government and industry. What are some "lessons learned" NCFTA can offer to government and other organizations seeking to establish and/or enhance alliances between government, industry and academia?

PLESCO: We're lucky in that before it became vogue or in fashion in government agencies to discuss the buzzwords of today or of tomorrow – information sharing and analysis centers, partnerships, etc. – we did it and we continue to do it. To do so effectively, it's all about credibility. Don't bite off more than you can chew. Do it for non-political reasons. Do it for substance and to share that information, not because there's political expediency in doing it.

My second tip is just do *something*. Initially, it took us literally three or four years to iron out what we were going to do. And then we decided, "This is crazy. What can we do? Let's just do something." We initially set up invite-only conferences to share intelligence related to spam threats. I actually wrote that research approach for the NCFTA before I was employed by the NCFTA; I was involved as a board member. I wrote that initial operation. That enabled us to sit down with industry representatives and FBI agents, think outside the box and use a task force to get to the next level to get a two-way sharing of information amongst law enforcement and the private sector. Identify what you can do effectively and just do it. Looking back, look more strategically at what were your achievable successes for the year and choose your resources accordingly.

From our standpoint, we're lucky to now receive public acknowledgement. We've traditionally tried to stay under the radar because of the entities we partner with. We help them stop fraud and save losses, etc. That's the role we want to continue to serve – threat mitigation and neutralization. Last year, unintentionally, we were named in President Obama's 60-day review of cyberspace. We were one of three entities cited in that report as knowing how to do information sharing from a public-private perspective. I really believe it should be a private-public perspective – not driven by the public sector, but driven by the private sector and what their goals are. It's our philosophy to share that information freely with our partners.

NSCI: Do you have any "best practices" where NCFTA's partnerships resulted in a result that might not have been possible by the organizations working alone?

PLESCO: Yes. We're currently funded 60 percent by private sector/40 percent by the public sector, but we're moving to be funded entirely by the private sector – through grants, etc. Since we're funded that way, I'll talk generally in sectors.

One very large brokerage firm came to us and informed us of the type of fraud they were seeing – a pump-and-dump fraud. It's the utilization of a customer account to artificially inflate the price of a commodity on the spot and then sell the commodity at a higher price, thereby creating organized crime where the bad guys can make money or the wholesale stealing of the money into people's accounts. This organization came to us and showed us what they thought was going on. We were able to bring in peer firms that shared information with us. Only through the sharing of that information and through

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **P a g e | 6**

cyber forensics analysis of the IP addresses that the firms were seeing and the botnets that were being utilized were we able to identify what was taking place from a strategic level and a worldwide level. It was targeting the sector as a whole. We wouldn't have seen that, but for our center and the trust of our partners to share that information with us. The information we're sharing is network forensic information.

NSCI: With all the technical complexities of cyberspace, how do you think we will get to a point where cyber forensics will result in information that can be effectively communicated to a jury and pass the court of public opinion?

PLESCO: You're asking a former prosecutor that question and it's a great question. At the end of the day, the judge and the jury have to understand in non-technical language what took place. The practical application of the theory knowledge, scientific knowledge or the network knowledge they have is so important. The ability to translate that into terminality and language that is understandable is key. To do that, the prosecutorial lawyer has to stay up-to-speed with the press, understand what they are, understand it in non-technical speak and be able to explain it to a jury. I'm not saying it needs to be dumbed down at all, but as a prosecutor, you have to understand the technology and be able to explain it through witnesses and through evidence collection in a way that a jury of your peers understands it and not a jury of systems administrators.

You have to do it from the perspective of an every-day user of technology, not as an engineer. We do a lot of that, for example, in this operation with the Haitian earthquake. We were instrumental in sharing information from experiences right after Hurricane Katrina and right after the tsunami.

At the end of the day, what are the risks? Risks from a corporate perspective track cyber threats from a systems or consumer perspective. These are sometimes very different, though, at the end of the day. Bad guys are trying to gain them for similar reasons. Understanding the technology and how it's being utilized to exploit the consumer is key. Consumers don't protect their machines; they don't keep up with anti-virus software. Because of that, bad guys exploit that. Explaining that in non-technical terms in how a crime can take place is key. Extrapolation of the current law into a technical environment is key to this as well.

NSCI: What initiatives is NCFTA currently involved in and how will they improve cyberspace security?

PLESCO: We're involved in an anthill on the financial front: the black market that exists for credit cards and brokerage fraud; threats to U.S. and non-U.S. consumers in dealing with that e-channel; and judicial issues with smaller banks – what are those threats? Those are three of the areas. The fourth is in pharmaceutical fraud: the sale and dissemination of stolen or counterfeit pharmaceuticals. With each of these, our industry and law enforcement partners are working together to involve academic institutions.

NSCI: Is there anything else you'd like to add?

PLESCO: Thank you for the opportunity.