ceocfointerviews.com

Issue: August 11, 2014
The Most Powerful Name in Corporate News

Cyber Security for Commercial and Government Entities

***Joe Church** - CEO*

About Digital Shield, Inc
Digital Shield, Incorporated (DSI) is dedicated to assist in the response, discovery, analysis, mitigation and tracking of cyber incidents as they occur within commercial and government entities. Digital Shield Security Professionals have extensive backgrounds in conducting forensic examinations, log analysis, network and physical security vulnerability assessments, and Certification and Accreditation requirements.

DSI Security Professionals are prior Law Enforcement Officers, both local and federal, prior military, and security engineers in large Fortune 500 Corporations. DSI Security Professionals have extensive experience additionally with International Investigations and have assisted government and commercial entities in areas such as North America, South America, Asia, Europe and the Middle East. All DSI security professionals hold a Top Secret or Secret Clearance.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

CEOCFO: *Mr. Church, your website indicated Digital Shield is your "Frontline in Cyber Defense," how so?*
Mr. Church: We give the client the ability to conduct not only investigations but also prepare for different types of attacks as they occur. We conduct front end assessments, which means we come in and assess the level of security on systems; and then mitigate any known weaknesses. We end up conducting full physical assessments and penetration testing to find any holes within a network that outsiders or insiders can use to gain access or steal intellectual property. We also have the ability to respond to incidents as they occur real time for our clients. We respond real-time to a suspected incident to be able to find out exactly what has happened and how the attack occurred, then are able to mitigate those risks and continue the investigation afterwards. All the people here that do our investigations are all certified forensic examiners, network examiners as well mobile device examiners.

CEOCFO: *What is it that you understand fundamentally about the process of security that allows you to be confident and to know that you are providing the best results?*
Mr. Church: It is hard for corporations to promote they have the best security solution for a client when they have not talked to the client to ascertain the current level of security implemented or asked the client what their security needs are or the type of information they are protecting. Solutions should be based on the client's needs and what is the client's mission. The reason we have been successful is we actually go out and meet to the client and find out what their needs are as an enterprise. We are then are able to build a solution around the results from those meetings. When people say they have the exact solution well that is a misnomer because you do not really know what the client needs until you go out and talk to the client, see their enterprise and see their weaknesses and strengths. The reason we have been successful is that we deal well with the client in finding out their needs and then catering a solution around their specific needs.

CEOCFO: *Who is the typical client?*
Mr. Church: We are a small company but we have the ability to respond to large corporate entities. We conduct Incident Response for small corporations or mom and pop shops all the way to Fortune 500 companies. We also conduct network based investigations/forensics for Fortune 500 companies. We provide a high-tech training solution as well; we train most of the federal agencies whether three-letter agencies or corporate entities. Many agencies out there have their own forensic units built into their corporation so they are looking for people who do this for a living, and live and breathe the technology to come out and train them on the latest technologies. The people that we employ and use out in the field are not just trainers but actively conduct cyber based investigations for a living and are embedded in this work. It is their passion. They conduct the investigations and bring all those different components from the investigation back and put them into the training courses that we provide so that students are getting the latest and greatest training.

CEOCFO: *What are some of the common areas that most companies do not understand about security or something out of the box that you can identify?*
Mr. Church: I think the first thing that companies need to realize is that you have to spend some money upfront to secure their infrastructure because it is much more costly to do it on the backend. When the Incident Response Teams come in

to try to figure out what happened, they will be paying a premium price and it may not be crystal clear how long the engagement will take, depending on the severity of the breach. The cheaper approach is to spend the money front, get the proper security assessments and penetration tests done. Test the network to find out where the holes are and mitigate them before they can be exploited. It is a cheaper solution than not performing the security tests and then all of a sudden a major incidence happens and you are putting several different units on the ground to determine how your infrastructure has been compromised. I think the misunderstanding may be performing these security assessments are very expensive but it is a lot less expensive then finding out you have a compromise and your client's data has now been leaked onto the Internet somewhere.

CEOCFO: ***Are people becoming more aware now because of the incidents at Target or are they still putting their heads in the sand?***
Mr. Church: I am starting to see a shift. Decision makers in organizations are starting to see incidents occur on a monthly basis and the news is now reporting more of the actual incidences as they occur giving an even greater awareness. I have been doing forensics over twenty years and traditionally many companies never reported these incidences. Compromised companies did not want their customers to know these incidences had occurred. They did not want their customers to say their data is not secure, and in response move over to another company. Recently we are seeing a lot more of these incidents being reported such as Target, PF Changs, etc. I believe there is a major shift in awareness not only for security professionals but also for the consumer. Many of the CEOs (Chief Executive Officers) and the CSOs (Chief Security Officers) are now saying if hackers are able to compromise companies like Target and PF Chang, then we are probably at risk as well and maybe we need to look at the network and find out if we are vulnerable.

"It is hard for corporations to promote they have the best security solution for a client when they have not talked to the client to ascertain the current level of security implemented or asked the client what their security needs are or the type of information they are protecting." - Joe Church

CEOCFO: ***Do you see a point when insurance companies would require a proactive approach?***
Mr. Church: We actually do some insurance work now for some of the larger companies. There are insurance companies out there that provide policies for these types of intrusions or compromises. Some of the insurance companies hold policies with some of the major corporations, so when there is a major incident these insurance companies now need the ability to have their own assessment done to be able to find out what the exposure is to the client. There has to be a third party that comes in for a major compromise to determine all the client's information that has been compromised so that they can actually serve notice to each one of those customers. Insurance companies are absolutely involved now.

CEOCFO: ***Would you give us an example of something that your people may have discovered that is unlikely others would?***
Mr. Church: Corporations have users now that are connected in with their mobile devices into the corporation's backbone and connect to the corporations WIFI access. There is what you call BYOD (Bring Your Own Device) into corporations. It is now causing a major issues because when employees brings their mobile device into the workplace they may have bypassed all the perimeter firewalls and protection that the company has actually paid thousands of dollars for. Many of these devices depending on whether it is Android or IOS are now being compromised. Android is probably one of the most compromised operating systems out there. As the employee brings their mobile device into the network, they may be opening up the network to major compromise if there is not a policy in place forbidding the employee from connecting to the corporations network. Everything now has shifted over to the mobile side and many employers have not yet found a solution to manage those devices when they come into the workplace. Many employees are bringing in their own devices and are not checking on whether those devices are being connected to the backbone and they are not putting up policies on how those devices are going to be managed. We specialize in mobile device investigations. We go a bit further by looking at the totality of the network and what devices are being brought into the network that are personally owned and how those devices can be managed.

CEOCFO: ***Where are the areas of the business that you see the most growth?***
Mr. Church: The area we are seeing the most growth in right now is the incident response and forensics arena because of the compromises that have recently come out. We are actively getting calls to respond to evaluate suspected compromised networks. The majority of our work currently is incident response. Depending on the compromise, clients may need additional services such network forensics/computer forensics or malware analysis to be able to find out how the actual compromise occurred. Training is probably about 30% to 40% of what we do. It is a good mixture because it keeps our responders entrenched in the latest real world procedures so we can reflect that information in the training courses.

CEOCFO: *What is the key to evaluating new technology?*
Mr. Church: I believe the key to evaluating new technology is to have an excellent research and development team. As new technology comes out, for instance Google Glass and wearable devices, you have to keep up to date on how the device works and how or if any data can be recovered from the device to use in an investigation. We try to get those devices as they come on the market and do research and development to build the best approach possible. We test the devices for any weaknesses and then we are able to post that information out on social media to make other people aware. We try to get that equipment or software in our hands and then we find out exactly what it does.

CEOCFO: *What surprised you over the years as the company has grown?*
Mr. Church: I believe the biggest surprise to me is the lack of concern for network and employee based training. Everybody always hears that you need to have good security measures in place but everybody thinks nothing is going to happen to him or her. They do not realize that hackers are not only out for information but sometimes they are looking for a place to use as a launch point. You have to be able to secure these devices to the best of your ability for the amount that your budget will allow. Another overlooked security measure is proper training of employees and what information they are allowed to disseminate. It is critical to train employees how to recognize phishing emails or social engineering attacks. You need to be able to employ people who have the proper knowledge to be able to lock these systems down and test these systems regularly. New attacks, viruses and malware are released every day and there has to be a supporting budget to be able to properly train, secure and purchase the latest and greatest equipment out there.

CEOCFO: *What have you learned from your law enforcement background that has been helpful in running the business?*
Mr. Church: It was a big shift because in being a detective and a police officer, you do not necessarily understand the skill sets that it takes to run a business. As a police officer you are put on the road and given a job and the tools to be able conduct that job. In a shift over to being able to run a business, it was a huge learning curve because I did not have the background of running a business and creating or maintaining my own budget. I had to learn about having money allocated to buying the latest equipment or being able to have employees and monitor them in real-time to gauge their knowledge and assign them to certain tasks. As a police officer, you are just given a job whether you are good at it or not. With owning a corporation, if you really want to be successful, you have to put the best people forward that have the greatest amount of knowledge in the technology that you are dealing with for a client. Therefore, you only have to send one person out that is good at what they do instead of sending three or four guys out that are mediocre or may not be good at all. I think the biggest thing that I have learned here is that when you treat the client right and you are able to give the client a fair and accurate price and you do the job exactly like you say you are going to, you will have a client for life because they will trust you. I have worked for other corporations that would say “YES” to every question a client would ask even if they did not have the expertise to perform that service. Then when the client calls for that service those corporations put employees on the effort that do not have the adequate skill set to perform up to the client’s needs. Those corporations started to get a bad reputation within the industry and everyone talks to each other especially many of these large corporations. When you do a job badly the first time, you will probably not going to get many calls back. That comes down to understanding the clients’ needs and putting the best people on that effort to make sure you meeting the clients’ needs and it is going to be done in a timely fashion. As a police officer, you are not exposed to that and you have as much time as you want to be able to make an arrest or to be able to track a person down. Within the corporate realm, everything is time based and you have to get certain things done within a timely manner and put the best people on the ground.

CEOCFO: *How are you able to keep up with the demand?*
Mr. Church: It is a constant effort. Sometimes it is feast or famine. What I mean is sometimes we are actually so busy where we have numerous guys that are all out at one time and nobody back at the shop being able to do that research and development. At other times, things are so slow where everybody is back at the shop. The hardest task is being able to maintain a schedule. Incident response is the hard part because you have to have people available 24/7 to be able to hit the ground running. We have to ensure the schedule always allows for somebody that is available to do that. We have also partnered with other small forensic businesses to share in the workload and for surge support. If we have an incident that comes in, and need additional people, we already have a solution in place with trusted partners.

CEOCFO: *Would you tell us about your foreign business?*
Mr. Church: We have done business overseas for probably the last thirteen years. One of the actual contracts we worked on is the US Department of State Cyber Training Program, which is the ATA contract (Anti Terrorism Assistance). Their mission is to train foreign allied law enforcement and military. These courses are anything from how the computer system works, all the way to doing advanced intrusions, network-based forensics and computer based forensics. We have been doing international work for the last thirteen years and we also get asked to provide information on different investigations that our former students are working on.

CEOCFO: *What will be different for Digital Shield a year or so down the road?*
Mr. Church: I think what will be different is the new technology that is coming out and being able to find a way to interact with the technology to pull information. There is now LTE which is cell phone based technology that is now is going to be

available in cars. You will be able to read your tweets and texts and take phone calls through the car systems themselves. As an investigator, you will now need the ability to go out and do investigations on new technologies like the car systems or the wearable devices. A technology pushes further into the future it is a constant race to keep up with those new technologies and be able to capture the information as well as being able to present it in a court of law.

BIO: Joseph Church is the President and Founder for Digital Shield Incorporated, located in Melbourne Florida. Digital Shield offers services such as Forensic Examinations, Incident Response, Vulnerability Assessments, Network Hardening, Certification and Accreditation, and Training for government agencies and commercial entities around the world.

Joseph Church is a former law enforcement detective from the Prince Georges County Police Department located just outside of Washington DC. Joseph Church was a Detective responsible for investigating and apprehension for crimes involving electronic evidence and hacking cases from Child Pornography to Advanced intrusions in Unix based systems. Mr. Church was also assigned to the Federal Bureau of Investigations (FBI) Innocent Images Task Force, where he tracked, traced and apprehended pedophiles across the Internet for Prosecution. Mr. Church later worked for Computer Sciences Corporation (CSC), where he was responsible for conducting training for the Department of Defense on Computer Crimes and Intrusion scenarios. Mr. Church managed CSC National Incident Response Team and Forensic team for conducting on-scene investigations for both internal and external client cases.

Mr. Church now consults for the Department of State Cyber Terrorism Training Program where he instructs allied countries Law Enforcement Agencies on how to assess computer crime scenes and conduct Cyber Terrorism Investigations while protecting evidence from contamination for courtroom testimony.

Digital Shield, Inc

2199 Rockabye Avenue SE
Palm Bay, FL 32909
321-704-1336 or 301-943-5456
www.digitalshield.net