ceocfointerviews.com

Issue: January 12, 2015
The Most Powerful Name in Corporate News

Confidential Electronic Communications for Businesses and Professionals

Mike Koclanes
President

CEOCFO: *Mr. Koclanes, what is the focus at Vaporstream™?*
Mr. Koclanes: It is a very straightforward value proposition. At Vaporstream we are passionate about protecting people's privacy in their electronic communications. We have developed the only solutions that ensure your confidential communications will not expose your company, your employees and your shareholders to unwanted exposure.

CEOCFO: *What do you understand about security that perhaps others do not?*
Mr. Koclanes: I think that the main perspective that we have is that, including my background, we are staffed with people who really understand the business requirements for secure communications. Many of the mobile applications that have come out were really consumer tools designed to try to make pictures or text disappear and they did not even do that successfully. However, we came from a background of data protection, data management, encryption, key distribution management; those types of things are required to do this in a professional manner, it takes a higher level of expertise.

CEOCFO: *What are some of the challenges in mobile that are greater or different from a laptop or PC?*
Mr. Koclanes: First of all, most of these issues exist on the desktop as well, which we support. However, in the mobile world, because your device is exposed you run a higher risk. You are on a variety of networks. You are changing from one set of networks to another; you might be on WiFi, then you might be on a cellular network. Your device is exposed and more susceptible to loss and or interception. There are even controls by governments within different boundaries to intercept or block capabilities. It is not as controlled as an internal corporate network environment behind your security firewall.

CEOCFO: *Are people or businesses really aware of how serious the nature of the threat is?*
Mr. Koclanes: I think that until very recently it has largely been ignored as a risk. I think that is largely because it was not understood how vulnerable they are. Then recent incidents, most recent being the Sony pictures exposure, where not only was there the reality of somebody hacking and stealing intellectual property, in this case the contents of scripts and film, but the emails of the employees and the employee's information were embarrassingly disclosed. It has become apparent that anytime you are digital recording anything, you run the possibility that information can be publicly exposed. In the past all of these digital communications left a trail, before Vaporstream. They leave copies of that email on servers, on devices, on other servers, on cell phones and on desktops. Those traces, that electronically stored information, are susceptible to be hacked and exposed. People were naïve enough to believe, "Well it is encrypted across the network." That keeps it from being intercepted. However, once it is received and it is decrypted and stored in so many different places, if someone gets into that network you are leaving that confidential discussion exposed. Therefore, I think the Sony situation and before that incidents like the disclosure of pictures thought to have disappeared from Snapchat but were posted publicly, have heightened the awareness. Recently the FTC cracked down on Snapchat, for example, because they were making claims that the pictures were disappearing and they really were not. All of those things heightened people to an awareness that, "I need to dig deeper. I am really not protected."

CEOCFO: *Who is coming to you for services? Is there a common thread among the businesses?*
Mr. Koclanes: It has now become a very broad cross section of companies and professionals. However, initially it was people who really understood that there was a risk if this information leaked out. Therefore, our initial customers, we would probably call them innovators and early adopters; people who were behind enemy lines in hostile territories, people who were working in locations where your phone could likely be confiscated by the government and you did not want to have your proprietary information left on the phone. They were the international companies, companies working with IP,

medical providers who were regulated to not disclose patient health information. Today our customers come from a wide variety of businesses including financial companies that are wanting to provide an extra level of protection when giving out passwords or account information or activation codes.

CEOCFO: ***What are your products? What are you providing and how do they work?***
Mr. Koclanes: Primarily, what we deliver is a streamed messaged platform that delivers the only truly ephemeral, temporary messaging solution. Prior to our solutions, everything that did electronic email or text messaging was a store and forward technology. Therefore, if you had a copy on your device it was forwarded to a server, which would forward to another server, which would forward it to a device. That was all because we were constrained. Our devices were not smart, limited in memory. The networks were limited in capacity. Therefore, every place that messages are left is a potential place for that data to be leaked. What we said was, "Those constraints do not exist anymore. Let us encrypt the message right on the original device. Let us encrypt it with a key that allows only the receiving person to be able to decrypt the body of that message. Let us just keep it in memory and keep it moving, so it goes from that device to our cloud and then down to the receiving device. When the person does see it, they decrypt it with their private key, so we cannot even see it. Then they can see the message and they have a chance to reply and/or just let it vaporize. There is not ability to store, copy, forward or paste, so it is fully contained. Only that person is going to see that message." Therefore, it is truly ephemeral. Most solutions that try to do this security just encrypt it when it is in transit. They store it on the phone. They store it on the servers. Then if you say that you want to get rid of it they delete it. Deleting it really does not delete it in most cases. It forensically still leaves it on the disk, so it could still be breached.

"At Vaporstream we are passionate about protecting people's privacy in their electronic communications. We have developed the only solutions that ensure your confidential communications will not expose your company, your employees and your shareholders to unwanted exposure." - Mike Koclanes

CEOCFO: ***Why should we believe? It seems like hackers can get into anything and many people claim to have the answer.***
Mr. Koclanes: That does make sense to me. What we are dealing with is that there is a basic lack of trust. Therefore, people are now saying, "I know I better not post something like that on Facebook. I thought Snapchat disappeared and then it did not really disappear and then the FTC cracks down on them." Therefore, people are saying, "Who do I trust?" What I can say is that the technology we have is patented. The patents have been issued, so you can look at the patents and those patents have been implemented. We can give references to our accounts and customers who have top security experts that audit our system. We actually do external audits with companies to come in and try to crack our system. We have had agencies of the government take phones that are using our application and try to get to the information on the phones and we passed those tests. We have people who are risking their lives if their phone is taken away from them and this information is found on their phone. They trust their lives with this application.

CEOCFO: ***What have you figured out? Is it being able to write the correct algorithm? What was the biggest challenge in implementing the concept?***
Mr. Koclanes: There are some technical hurdles that are the secret sauce, if you will, that are in the patents around the concept of, "How would you do this if you were going to do this right from a key management, key distribution, and encryption mobile development methodology." Those are technical. Actually, the real breakthrough, I think, was just the timing of us thinking that there is an industry need for this. All of the apps that we saw out there were basically toys. We saw an industry change that said there is enough bandwidth to do this in volatile memory only. There is enough power on the receiving devices that you could do it in memory on those devices. There is enough capability and if we do the right encryption algorithms and key management to put all of those together and not have the same barriers that we had in the past. If you think about it, when I was a younger man we used to share the same phone line with our neighbors. They were called partly lines. Part of that was because we could not afford our own separate bandwidth for every house. It seemed totally natural to ask your neighbor to get off the phone so that you could make a call. That was constrained. We had constrained bandwidth and only had so much capability. If you were to design it today you would not do it that way. Email was probably the most vulnerable of all of these things. These technologies were developed twenty and thirty years ago. We just looked at the industry as it looks today and said, "With the capabilities there today how do you solve this problem in a professional fashion?"

CEOCFO: ***Would a company typically be using this solution across the board? Would they save it for specific instances? What is a typical implementation?***
Mr. Koclanes: That is a good question. Usually, it starts out with some perceived risk or need in a portion of a company; often at the executive staff. They have got people that are on the road. They are travelling all over. It is just logistically a

nightmare to try to do face to face meetings and phone calls for confidential conversation. This is the kind of stuff where you say, “If I have this conversation it is going to be face to face. I do not want this IP or this product idea or strategy or feedback leaking.” Therefore, often it starts out with the executive team, sometimes the CEO to CISO team and the CIO team. Then it expands, to how do we deal with the cyber threats themselves and communicate across the company when our systems might be compromised. Then to corporate development teams that are dealing with M&A discussions, then product teams, legal teams and HR teams. Those are often the first ones. We will usually start out with twenty-five to fifty people within a company. They quickly begin to realize that this is really straightforward to deploy and straightforward to use. They realize they could open this up to any employee who wants to communicate anything confidentially, employee to employee. Then they push the application to all their desktops and devices.

CEOCFO: ***Why not just use it overall for everything? Is it taking up too much space somewhere? Is it too costly?***
Mr. Koclanes: It is not costly. It is cheaper than the mail system, we use no storage. However, there is a purpose for when you do it and there is a purpose when you do not. We are not the end all. We do not say that we are replacing email. If you want that person to actually have something so they can forward it to their team or you have something that you want them to keep for later reference, if it is not something that is confidential, email works fine or text might work fine. This is really for more temporary, private communications; things that you want to communicate to them and make sure that they are the only ones who have it and that you are looking for a responsive answer; that is the appropriate time for this. It is often when you would stop and say, “I am not going to put this in email, I am going to give them a call.”

CEOCFO: ***How does it work different than email? What would someone do when they want to use your system as opposed to sending an email?***
Mr. Koclanes: It looks very similar. You would have an icon on your desktop or your phone for Vaporstream. It pulls down an address list of the people that you have Vaporstream connections with after you integrate it into your corporate directory and so on, for other people that have Vaporstream. You select the people that you want to send it to. You put in the subject and you put in your message or attach your PDF image or whatever and you hit send. Therefore, the learning curve is almost zero. It feels like you are kind of sending an email. You receive it. You see it in your in-tray from the person. You click on a “message from Mike” for example and then it shows you the body of the message. It never shows you on the screen the body and the header information, the from and the to and date/time at the same time. The reason for that is the screen shot would not have context, and it has actually been held up in court, that a screenshot it is just hearsay. Therefore, it is just like a voice conversation. It is ephemeral. It was only in memory and you have no record of it. Therefore, you see it then and you can hit reply or you can let it vaporize. In either case, after you hit reply that original message vaporizes. You now have a new message, which is the reply to the original sent message.

CEOCFO: ***Would you tell us about your disaster recovery feature?***
Mr. Koclanes: We have got a couple of different options on the product. One thing is called the Information Governance Module (IGM). In some regulated industries, even with these confidential messages, you need to keep a record that you sent it. The point that we are making is that the messaging system and the devices should not be a record or be a point of potential data breach. Let me give you an example. A doctor has a test result. They are going to send that test result to the patient. They already have a secured record in the patient medical records system of that test result. They do not need the cell phones and the servers in between to have another copy. Therefore, to protect PHI, Patient Health Information, they send it with a Vaporstream. It gets received on the other end. They are confident that only that patient can see it and after viewing it is gone. They are not going to accidentally leave it somewhere where that patient information gets exposed. If they ever needed to go back and recheck they can always get into the patient medical record system. If you do not have such a system of record we can supply the IGM module to provide a message archive encrypted behind your firewall and not in the messaging system or devices.

CEOCFO: ***How are people finding out about Vaporstream?***
Mr. Koclanes: We are trying to get the word out through talking to appropriate information sources, such as your magazine. We do pretty active blogging, the Vaporstream website and Twitter pages and through LinkedIn. We are attending corporate events dealing with these types of issues, such as LegalTech at the beginning of the year and also on a number of radio campaigns on shows that talk about security and cyber protection.

CEOCFO: ***Are you funded for the push? Are you seeking partners or distributors?***
Mr. Koclanes: The company is privately held by a number of large investors. We recently closed an additional $5M round in funding. These are people in the insurance business, pharmaceutical business and other industries. We do sell direct to businesses and professional. Some individuals find us through our web advertising and contact us directly. We also have some channels that do sales for us in specific verticals, medical collaboration systems, security systems or mobile device

management systems. Also you can get a free trail downloading from the Google Play and Apple appstore, search for Vaporstream.

CEOCFO: ***What has changed since you had the concept? What have you learned as the system has been in use?***
Mr. Koclanes: Most of this is based on customer feedback. We have learned, at the executive level, that the experience has to be such that there is virtually no change management, no training required; if they cannot pick it up and use it within the first five or ten minutes, we know they are not going to use it. Therefore, you have to make it familiar to them in terms of the way that it is used. The second thing we have learned is that people cannot really appreciate it until they use it. In other words, it seems so simple but often they say, "I do not know if I have anything all that confidential." Then after they get the application they immediately start realizing all the times in a day that people communicate confidential or transitory information by email or text. "What is my password or account number?" or "What is the flight information for when we are leaving on Thursday?" It is not really safe to send that information by email. Finally, you can load Vaporstream so that if you are using your tablet, Macintosh, PC or cell phone, and notifications will go to all of those devices that you have a Vaporstream message or Visper. You click on it and see it on the device you are using. Furthermore, if you are trying to reach perhaps a doctor who may or may not be in the building, you do not have to figure out, "It is after hours, you have to page him; it is during hours, I have to call him, he is travelling you must email him. You do not have all of that complexity. You just Visper them and it will reach them, whether they are on Wifi, whether they are on cellular and to whatever device they are on.

CEOCFO: ***Why choose Vaporstream?***
Mr. Koclanes: Why Vaporstream? It is because we are the privacy experts. We are the only one who came at this from a business standpoint. How do I protect the information in my confidential communication and protect my employees, my co-workers, my shareholders and be confident when I communicate electronically that it is safe and will not reappear unexpectedly.

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

For more information visit: www.vaporstream.com

Contact: Michael P. Koclanes 312-380-5348 mike.koclanes@vaporstream.com