CEO CFO

ceocfointerviews.com
All rights reserved!
Issue: September 7, 2015
The Most Powerful Name in Corporate News

InfoGPS NETWORKS, INC.

Information Governance Software that allows Organizations to Track, Monitor and Classify Data in Real Time

Paul Hugenberg III
Co-Founder and CEO

CEOCFO: ***Mr. Hugenberg III, what is your approach at InfoGPS Networks? How are you helping companies be more secure and avoid risk?***
Mr. Hugenberg III: The basic risk argument that every company attempts to address as it spends dollars on security is to prevent an outside intruder, a bad actor, from accessing information that is stored inside their network, their private data, and removing it. We commonly call that a data breach. InfoGPS, at its most basic level, allows organizations to view all of that information by using software that tracks and monitors in real time. It that respect, they can protect it by spending dollars in a targeted fashion.

CEOCFO: ***How are you able to really do it at InfoGPS? What do you understand that others may not?***
Mr. Hugenberg III: We have a basic philosophy that is grounded in principles of financial risk and information technology risk; that is, identifying the key driver of risk is the most important step in any management scenario. What we try to communicate and educate the market on is that information is the driver of risk. Therefore, when we attempt to identify our breach risks, whether they are technical or operational, we start with the basic questions, "What are we using the systems for (what information is needed), who needs that systems if there is a disaster (what information must be available), what type of information are we storing on those systems (is it sensitive) and is there a risk to us if it is lost (what will it cost to replace or notify impacted customers)?" These basic questions tell us that information is the fundamental keystone for identifying risk, no matter what system we are looking at. Therefore, our goal is to use software to run through literally the millions of files that exist on a network and expose, not only to index the contents of those files, but specifically target where information is regulated or sensitive to the organization. More importantly, we classify and risk score each record and communicate where there are concentrations of data in the network. That is very important, because that is where the breaches occur and most organizations are unaware that it is present.

CEOCFO: ***Do companies always realize the data that is important or are there areas that companies might not realize should be considered of consequence, as down the road they may become so?***
Mr. Hugenberg III: Absolutely! What we see is, again, not only in technology, but across almost every discipline in business environment, we become embedded in our habitual routines. Whether we are talking about financial statement risk or talking about system risk, most of us approach it in the way that we always have. Most of the consultants that we bring in also ask us the same questions, assign risk or perform their audits in the traditional manner. What we know from actual breach reporting is that this approach in incomplete. In fact, our enhanced approach has exposed some common control gaps in companies who report a breach. These gaps are a result of managing risk using outdated approaches. First, there is a noticeable gap in a business's understanding as to where their sensitive data lies. Second, the compromised information always unstructured, which means it is information that is exists outside of our primary applications. Next, this unseen information is always in places on our networks that we own, but are dark. In other words, we do not have visibility into those areas using traditional controls. Finally, it is nearly always regulated or non-public information. This final point is significant as it exposes the organization to financial and, at times, criminal liability.

CEOCFO: ***Would you explain the monitoring data at rest concept?***
Mr. Hugenberg III: On almost all commercial networks, information has to exist at rest at some point in its life cycle. At rest just means that it is stored somewhere. It is saved on a file, saved on your computer or saved in an email. The

monitoring portion of our software looks to identify and classify information every time it is created, stored or deleted, capturing it as it becomes at rest. As soon as we find it we do perform our interrogation and risk ranking in order to ensure that monitoring occurs all the time and continuously. This gives us the ability to help our customers understand what their information risk posture is as of the moment they run a report.

CEOCFO: ***What should a customer be doing at their end to mitigate some of the risk? Do you work with them on things as simple as not using a very easy password or making sure that when people leave their clearance is taken away?***
Mr. Hugenberg III: That is a fantastic question! Again, there is nothing particularly special about information technology and system risks and how to protect them with layers of controls. If you want to keep someone out of your house you may lock the door, but you also may lock the windows. Perhaps you would install an alarm or buy a dog. Those are three or four different layers that are in place to help you keep somebody out, and also inform you some of the layers have been compromised. System risks are all the same and include many layers. We do work with our customers to isolate where their sensitive information is stored. Next, we have a conversation and help them make better decisions about missing controls or misplaced controls. Remember, we do it from the key point of inventorying the data risk first and then having a conversation with them about applying controls to that risk second.

"What that means is almost ninety five out of every one hundred dollars we spend is focused on protecting assets that we haven't even taken the time to discover. That is our biggest problem. Many experts in the IT Security arena believe that this misalignment, or rather, ignorance of the location and sensitivity of data assets is responsible for 75-100% overspend in on security software."- Paul B. Hugenberg, III

CEOCFO: ***Who is coming to you for services? At what point might a company realize that they should be taking that next step and really paying attention to what you can provide?***
Mr. Hugenberg III: That is an interesting question. Generally, industries that have a regulatory oversight or what we call highly regulated industries. Those would be banks, hospitals and credit card processors. They have a pretty mature structure and are audited frequently. Those are our general customers. Where we find the most traction or where people are the most excited about what we do, unfortunately, is after they have had an issue. Within any of the various local, state, federal laws, and/or regulations are two requirements. The first requirement is to take the necessary steps to inventory and classify information before anything else is done. The second is after you have suffered a breach, or potential breach: identify all of the records that have been stolen, and then contacting each person and letting them know that their data might have been stolen. That can a very expensive, time consuming and often inaccurate process for organizations. Therefore, once they get breached there is a real sensitivity to, "What do I have and can you help me figure it out so I do not have to suffer through this again." A very simple exercise to perform this post-breach triage can cost a small organization upwards for $50,000. For many, that is an expense that can affect their ability to survive the event.

CEOCFO: ***So much is done these days through online search. What do people look for when they want to find your company? Are there one or two category identifiers? What is your company's designation?***
Mr. Hugenberg III: Our Company exists in a space that is generally called data governance or information governance, depending on the author. It is sometimes referred to as data interrogation. We do much more than the process of interrogation, but that is the umbrella that we would fall under.

CEOCFO: ***How are people coming to you? Is it word of mouth? Do you do conferences? Is it a challenge to get people to understand the importance of what you do?***
Mr. Hugenberg III: Our biggest challenge today is education. Historically, there has been roughly seventy billion dollars spent on IT security in the United States alone. This is spent on typical controls that may include passwords, firewalls, antivirus, log analysis, auditors and things like that. New software comes out every day that tries to do all of those same things, only better than the last one. Only about five or six percent of that seventy billion dollars is focused on data governance. What that means is almost ninety five out of every one hundred dollars we spend is focused on protecting assets that we haven't even taken the time to discover. That is our biggest problem. Many experts in the IT Security arena believe that this misalignment, or rather, ignorance of the location and sensitivity of data assets is responsible for 75-100% overspend in on security software. A few question ago we spoke about how people determine the expectations of their control structure and spend money in a habitual way. Industries have really believed and entrenched themselves in the concept that, "If I build higher walls and those walls are thicker and I put guards at the door nobody can get in, so my treasures are safe." What we have found in the last four consecutive calendar years are a record number data breaches by companies that have very high walls and very thick walls and very few doors that they know about. Therefore, we have

a lot of education that we have to go through to get our customers to understand, “Let’s start at the beginning so that the rest of your spend is affective.” That education puts at conferences, on panels, in whitepapers, and in front of companies in trying to indentify partnerships where we can marry up with one another and help them do their job better. Honestly, it is knocking on doors. The more we talk about our product and what we offer the better we get. We have been happy to see some increase in our sales efforts and it is a result of all of those things; continuously talking, continuously educating.

CEOCFO: ***What have you learned since the company started in 2013? What has changed or what is different/better today than when you started?***
Mr. Hugenberg III: There are two answers to that. One is; the industry, both from a regulated side a legality side, has an increased awareness of the amount of data that is being lost and is hidden on their own networks. President Obama has referenced cyber security in his state of the union speeches two years in a row. We have a federal cyber security czar that has been appointed, and cyber warfare is now considered a domain of war. We have regulation coming out in the banking industry that is asking banks to share information about security events to make us all better. We like to say is that we were the precursor. We were here before it was sexy. We were country before country was cool. However, the industry has certainly caught up to us and we are glad to see it. The second thing that we had to learn, and we spoke about just a minute ago, is the time and effort it really takes to pull folks out of their entrenched positions on how to spend security dollars. That is a very, very tough and sometimes long conversation.

CEOCFO: ***When you are talking with a prospective client can you tell if they are really receptive in the beginning?***
Mr. Hugenberg III: We can tell right way. We normally tell within about the first thirty seconds. It is usually a head nod or note taking, and often it is a direct interruption as soon as we start talking. “You can do this? Really, you can do this? What does it mean when you say you go search,” and it becomes a very interactive conversation. Conversely we know very quickly whether or not that conversation is going to be one of those education conversations, where we are probably not going to sell something today, but we have the opportunity to tell our story and try to leave a seed or a little bit of a nugget of behavioral suggestions to that client.

CEOCFO: ***Are you able to help companies that do not have a large budget? Are there layers or is it an offering that really needs to be embraced in its entirety?***
Mr. Hugenberg III: Yes, we can help companies of all sizes. The beauty of our solution is also in its simplicity and scalability. The majority of companies in the US are small businesses; we are about four thousand dollars a year, for continuous oversight. It is a fantastically affordable solution for most banks, doctors’ offices, law firms, CPA offices, retail outlets. For those customers who have the most risk, the largest networks and significant amounts of customer information, we have built our product in a fashion that we can scale from 1 or 2 computers to 100,000 machines.

CEOCFO: ***Why choose InfoGPS Networks?***
Mr. Hugenberg III: InfoGPS is really the only security oriented software available to you today that is built by IT security professionals as opposed to software companies trying to fill out a service portfolio. What we are doing is solving a problem that we had and not necessarily picking a line out of a law and trying to craft a solution to meet that black and white requirement. There is really a business opportunity here, a business awareness that we bring that our competitors absolutely do not. Secondarily, we are a product of the new technology set. We have a very affordable, low overhead, easily installed product. The competitive solutions in the market that have been around for a while are very heavy, with significant costs in hardware and software and licensing. We are a very friendly, light weight, easy company to deal with. At the end of the day we give you exactly the answers that you need to do your business better. If we can do that we will continue to be successful.

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

InfoGPS
NETWORKS, INC.

InfoGPS Networks, Inc.

For more information visit:
www.infogpsnetworks.com

Contact:
Paul B. Hugenberg, III
330-639-0009
paul.hugenberg@infogpsnetworks.com