Issue:
September 30, 2013

CEOCFO Magazine - The Most Powerful Name In Corporate News and Information

The Leading Global Cyber Threat Intelligence Firm, iSIGHT Partners Delivers Intelligence Products and Services to Public and Private Sectors, Providing Detailed, Actionable Intelligence Essential to Comprehensive Security Strategies

Technology
Cyber Threat Intelligence

iSIGHT Partners
8333 Douglas Avenue, Suite 1460
Dallas, TX 75225 U.S.A.
214-731-4585
www.iSIGHTpartners.com

John Watters
CEO

BIO: John P. Watters is currently Chairman and CEO of iSIGHT Partners, a Global Cyber Intelligence company based in Dallas, Texas. Prior to iSIGHT Partners, Mr. Watters was Chairman and CEO of iDEFENSE and an active investor in leading security companies such as TippingPoint, Archer Technology, where he served on the Board of Directors, and Netwitness, where he served as Chairman of the Board. VeriSign acquired iDEFENSE in July 2005 and Watters launched iSIGHT Partners in 2007.

In the 15 years before entering the cyber security industry, Mr. Watters was Chairman and CEO of several large diversified investment companies managing principal investments totaling more than $300M. He has served on more than 20 corporate and non-profit Board of Directors and is currently Chairman of Andromeda FC, a United States Soccer Federation Development Academy, Founder and Chairman of STAIRS Foundation, providing inner city children enhanced academic training in order to earn scholarships to elite private high schools in Dallas, and serves on the Investment Committee of The Jesuit Foundation in Dallas. Mr. Watters graduated from Santa Clara University, attended the London School of Economics, and is married with five children.

About iSIGHT Partners:
iSIGHT Partners is the leading global cyber threat intelligence firm, delivering intelligence products and services to over 150 public sector and commercial entities. We provide Fortune 100 companies with detailed, actionable intelligence essential to a comprehensive security strategy. Whether you are interested in our ThreatScape® intelligence products, our ThreatSPACE® cyber range or our ThreatServices, iSIGHT Partners can make sure that your company has the intelligence needed to protect its valuable intellectual property.

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: Mr. Watters, what is the concept at iSIGHT Partners?
Mr. Watters: Intelligence leads operations in every aspect of military doctrine. Why should cyber security be different? Our public and private sector is under attack from adversaries all over the world with a variety of objectives ranging from stealing IP to stealing money. Many companies don't have any idea who they are up against, what their capabilities are, and how they are targeting them. At iSIGHT Partners, we change the risk calculus and provide our customers risk decision advantage over their adverseries. You would not go into a fight unless you knew the adversary's capability. This allows appropriate resourcing against the adversary. Today, the commercial sector is recognizing that they are up against the same cyber threats that the government has faced for years, yet they have approached the challenge very differently. DOD spends more than ten percent of its cyber security budget on intelligence programs to determine how they invest the other ninety percent to counter the threat. The first ten percent is spent to understand the adversary's capability and the other ninety percent is deployed to counter the threat. The private sector has spend more than 98% of its cyber security budget on people, process, and technology to instrument its environment prioritized through a regulatory and compliance lens. They have sprinkled around less than 2% of their budget to make sense of the mammoth number of security events that they are fighting. As the private sector looks forward, we have seen a significant focus and priority on building an intelligence program that helps them understand their cyber threat landscape and deploy their security resources to

counter the threat and address the highest risk. Therefore, we see a major growth opportunity as the commercial sector is recognizing that they need to invest a substantially higher percentage of their overall IT security budget to build an intelligence program and secure a world class cyber intelligence partner to help them maintain insight into their threat environment. As the overall growth rate for security spending matures and slows over time, we believe there will be a substantial reallocation within budgets as the private sector drives intelligence spending from 2% to 10% of their overall cyber security budgets and ensures efficient allocation of the other 90%. Modest efficiency gains with the vast majority of your security budget will more that outweigh the cost of the intelligence program. This shift into intelligence led security will create a 50% CAGR of spending in the intelligence sector, in which we have secured the leadership role in.

iSIGHT is the global cyber intelligence leader that works closely with both the public and private sectors aligning security operations and technologies with the business and risk. An efficient intelligence program enables customers to prioritize security resources to counter high impact threats.

CEOCFO: What surprised you most as the business has grown and developed?

Mr. Watters: That it took this long for people to recognize that there is a better way? It amazes me that it has taken this long for executives to finally ask the question of their security organizations: "Is there not a more efficient way to manage risk for the organization than what we are currently doing." Instead, they have just thrown more money at the problem. Companies were stuck in their way of discovering vulnerabilities and focusing efforts based on exposure rather than threats. At some point they realize that if you try to prevent everything, you protect nothing. The goal of security organizations has historically been primarily concerned with compliance with the regulatory frameworks in their industry. Security organizations were not focused on countering threats and managing risk. We have seen a recent change and the thought leaders are quickly moving into an intelligence led approach to security. It appears that we are moving from the bleeding edge to leading edge in the cyber intelligence sector. Until recently, the vast majority of companies have operated without an eye towards the adversary, their capability, and how you counter it. While this is baffling to me, it is also the reason why I see such incredible opportunity for the industry. We saw a major need in the market and invested to create our unique intelligence capability at a time when other security companies were trying to tweak a broken system.

CEOCFO: What are some of the common or more recognizable ways that you provide protection?

Mr. Watters: Looking at cyber security through a sports lens simplifies the approach. Essentially, we build playbooks on adversaries that are targeting our customers. We then deliver the 'audibles' associated with these playbooks in order for customers to preposition defenses against the adversary. When an adversary says "367 Blue" the defender knows the play and initiates the appropriated defensive scheme. In cyber speak, this analogy is relayed in terms of attack methods and technical indicators– the audibles. In essence, we help customers find signals in the noise of their security operations and shrink the problem to a manageable number of threats that their internal cyber defense team can actually deal with. The problem in the industry is that there has been such a flood of traffic from adversaries that no matter how sophisticated internal security organizations are they are only able to shrink the problem from what are literally tens of millions of security events to perhaps a thousand critical events. The reality is that their teams can typically only deal with a very small percentage of these 'critical' events. Therefore, it begs the question, which events do you deal with? This daily decision highlights an important role of intelligence. When you are able to correlate an incident indicator/security event with the intelligence indicator associated with the context of the actual threat, prioritization becomes simplified. For example, a critical event may point to a specific piece of malware. Correlation of the malware with advanced intelligence will illuminate that the particular malware that has been executed against you is connected to a specific cyber espionage campaign targeting your sector for strategic advantage. Connecting the event data to the actual threat behind it enables a fundamental assessment of the impact of a particular threat to your organization, thus enabling a prioritization of your tactical and strategic security resources to counter high impact versus commodity threats. As we study the adversary, the infrastructure they use, and the playbooks they execute against our customers, we connect the technical indicators to our intelligence reporting and the associated "playbooks." Therefore, a customer knows, "If I see this IP address and it is dropping this indicator, then I know that it is Adversary 'A' that is executing a criminal strategy against me to steal customer credentials. This important linkage enables customers to quickly shrink the problem and focus their incremental resources on the highest impact threats to their organization. Absent a linkage between critical event data and the context of the threat, defenders are flying blind.

"An intelligence led approach to security requires world class intelligence fused into your security technologies and operations within a prioritization framework grounded in economics." - John P. Watters

CEOCFO: Is it all in the software? Is it all in what you have figured to identify and what the programs could put together? Is there a human component that says, "Maybe it does not match everything, but somehow I think it is a problem"?

Mr. Watters: The answer is all of the above. We sell adversary insight delivered through ThreatServices, ThreatScapes, and iRIS, our patented iSIGHT Risk and Intelligence System.

The delivery of this adversary insight is through annual subscriptions to our cyber intelligence products that produce a recurring flow of intelligence information with the associated technical indicators. These technical indicators are essentially anything that a security device can read that is associated with a high impact threat. The critical value lies in the linkage between those intelligence indicators that were found through our global intelligence efforts to what you are experiencing in your security operations. Without the link between the indicator and the threat context (audible and playbook), security operators have to take comfort assuming they blocked something bad, which is insufficient to validate and defend the investments that are being made into security organizations. Unless you can quantify the impact of the threat that you detected and defeated, you cannot even start to quantify ROI. In short, the only ROI in security lies in the avoidance of impacts. You would spend $1 to avoid a $100 loss but would not spend $100 to avoid a $1 loss. In order to assess the efficiency of your security organization, you must be able to link the security investments you make in people, process, and technology to the impacts that were avoided by virtue of those investments. Therefore, a key value of intelligence lies in the monitoring of the adversary's infrastructure and their activities to determine their "known bad" indicators are and link these to the associated playbooks. If you look at this approach through a sports analogy; the security defenders do not even know what teams they are playing or which sport they are playing. The technical indicator would be an audible – "635 Blue". The linking of audibles to playbooks to scouting reports enables defenders to shrink the problem and focus on what matters. Out of a hundred million events, your advanced technologies should dramatically shrink the problem. However, I have yet to meet a security organization that is able to use technology to shrink the problem to a number of critical alerts that are equal to or less than the number their organization can handle in a day. In fact, it is more typical to find an organization with 1000 critical alerts and staff to deal with 10. The question is which 10 do you focus on? Linking threat indicators and the associated context to the 1000 allows your security organization to focus on the 10 that really matter. That is because they are connected to high impact delivering threats, not noise or low risk threats.

CEOCFO: You recently announced a patented technology for security implementations based on business impact. Would you tell us about that?

Mr. Watters: Absolutely. iRIS, the patented technology you reference is a game changer for the industry. As alignment of security resources against high impact threats is critical to an efficient security organization, we focused on helping customers make that determination at machine speed. While the core patents were filed over the past 4 years and all issued this year, the combination of the patents are reflected in our new iRIS Product. iRIS stands for iSIGHT Risk and Intelligence System. This system contains our threat intelligence information with all of the associated indicators and creates what we call a "threat register". A threat register entry would be, "Group A with a high level of sophistication is targeting banks for wholesale theft of on line banking credentials." An organization can assess each threat register item and determine what the impact is to their organization. "Would that event be a ten million dollar event, a million dollar event, or a non event?" By allowing the customer to uniquely ascribe an impact value to their organization of a particular type of threat they begin to focus on impact avoidance rather than security events. As I described earlier, the intelligence indicators that relate to that threat register item are contained in iRIS and the specific technical indicators associated with the threat are linked to their security infrastructure. Therefore, a security event can now connect to a clear impact value to their organization. Today, Security Operation Centers and Incident Response teams tactically make decisions and "fight fires" without any orientation around the impact of a particular threat to their organization. They could be fighting a really mammoth fire or a small dust fire in the corner – they don't have visibility. iRIS allows them to know that a particular indicator or threat is connected to a major fire. Fight that one first. A different indicator is connected to a small fire; fight that last. In summary, the patent portfolio covers a system that maps intelligence indicators to the customer's incident indicators (event data) and drives a decision platform geared around real time business cases. This system provides a clear connection of security organizations to the company or agency that they are protecting. This fundamental alignment is desperately needed in the security industry and we are passionate in helping leading cyber security organizations align with the business. iRIS will help bridge the communication chasm that exists between security organizations and their leadership.

CEOCFO: Have people tried to create such a measuring scale before? What has been the history? How have you been able to create it when others have not as efficiently?

Mr. Watters: That is a good question. The simple answer is that statisticians and risk professionals have tried to tackle this equation before absent access to cyber intelligence and have failed. They have tried to build precise analytical models and have lost the forest through the trees. Perfection and precision is the death of security. In reality, we are dealing with a problem that requires and expert system to address. I laugh when wonderful minds try to defend the probability of an attack down to the decimal points. In essence, there are 5 key variables in calculating the risk per $ of investment in security and 4 are knowable within an expert system. Threat, Countermeasure Program Effectiveness, Impact Value, Investment Level by Countermeasure Program, and Probability of an Impact or set of Impacts. Active and likely threats against your enterprise are knowable within reason. The effectiveness of a certain countermeasure program are knowable within reason so long as you have the 'playbook' of the adversaries that you're up against. The investments that you have made in each countermeasure program are knowable or you are definitely "fireable" as a CISO.

Impacts are generally knowable on a scale. In all of these categories, the key is to create a scale for each category, not an exact value. Let us assume a 1 through 5 scale for threat intensity, countermeasure effectiveness, impact value, and investment level. The current probability of your composite threats penetrating your current countermeasures and delivering high negative impact to your organization is not knowable. We simply equate the probability as "X." What can be forecast is the direction of probability. For example, if you are protected against a particular attack and we see your adversary successfully testing higher level capability and chatting about targeting you, then the probability of the specific impact of that threat has increased. In short, the critical logic underlying the technology is laced in economics and resource scarcity. Given the changes in the threat environment that I operate in, the relative impacts of each threats, and the relative cost to enhance a countermeasure program to counter each threat, where should I put my next $ of investment? That is the simple risk calculus that is embodied in iRIS. At the patent review earlier this year, the reviewer said that our discussion was the best interview that she had in fourteen years. In the 2 days prior to our meeting, she interviewed six new security technology companies describing how their unique security technology would generate another critical security alert and/or block. She said, "You are the only firm focused on determining what that alert means to me." The elegance behind our approach and technology is the simplicity of it. Prior to the last decade in the cyber security industry, my background was using my finance and economics background as a principal hedge fund and private equity investor. A fundamental economic principle lies in the allocation of scarce resources. In order to optimize scarce security resources, you need to know what the best incremental decision is at all times. The only way to make optimal decisions in security is to understand what impact is connected with the threat that you are facing, so that you can apply your incremental resources to the highest impact threat first and the lowest impact threat last. An intelligence led approach to security requires world class intelligence fused into your security technologies and operations within a prioritization framework grounded in economics.

CEOCFO: You mentioned that you work with governments as well as with enterprise. How big a role is the government business? Do you see it growing? Would you like to see the mix changing?

Mr. Watters: Historically, our business has been equally split between the public and private sector. Prospectively, we see the private sector leading our business into the future. All of a sudden, it seems like executives are coming to grips with the reality that they cannot continue doing the same thing over and over again and expect different results. There has been an awakening among CEO's, security professionals, risk organizations and boards of directors that the cyber threat environment that they operate in has changed dramatically and they must change as well to protect their most valuable assets. iSIGHT Partners is far and away the largest and the most successful cyber intelligence company in the world and we are well positioned to lead the industry into intelligence led security.

CEOCFO: How do you reach your potential customers?

Mr. Watters: In the first five years of our business we did not have a sales effort. It was literally word of mouth. We did not have a marketing program and did not have a sales focus. Over the last year we have begun to build out a professional sales organization to embrace the demand. Many of the leading security analysts recognize this fundamental shift to intelligence led security, referred to as Cyber Security 2.0, and are bringing focus to the sector. Therefore, many organizations are now reaching out for an intelligence solution only to realize that there are more fakers than highly functioning cyber intelligence companies. As we have been exclusively focused on building our cyber intelligence capability over the past 6 ½ years, we have significant first mover advantage over the newcomers, most of which are leading with a technology solution claiming to deliver 'intelligence.' The vast majority of our resources have been spent on building a world class intelligence capability. Over the past 2 years, we began to build iRIS to help customers quickly deploy intelligence led security programs. As iRIS enters the marketplace in '14, the market is poised to accelerate its transition from a Cyber Security 1.0 to 2.0 world. You will also see many recent press releases around our technology partnerships that we are executing enabling our customers multiple approaches to match our intelligence with their various security technology partners. We are intelligence driven, technology neutral, and customer centered. We wake up every morning in our customer's shoes.

CEOCFO: What are the differences between your product offerings?

Mr. Watters: We sell threat intelligence products branded as ThreatScapes, ThreatServices in the form of threat and breach diagnostics to help customers understand their threat reality, ThreatSPACE which is our cyber range capability for training, and iRIS, our iSIGHT Risk and Intelligence System. Simply stated, we help customers diagnose their threat reality through an analysis of their recent security event data, deliver intelligence products to help them maintain adversary insight into these cyber threats and will soon allow customers to connect our intelligence to their security technologies and drive prioritization based on impact.

CEOCFO: Why should investors and people in the business community pay attention to iSIGHT Partners?

Mr. Watters When fundamental change is occurring in an industry, investors and the business community are always attracted to those visionaries that saw the change coming and took the risk to build capability to intersect the future. That is exactly what has happed with iSIGHT Partners. It is a tribute to Blackstone and our investor group that they are focusing their investment efforts to take advantage of this major industry transition and view iSIGHT Partners as the cornerstone of Cyber Security 2.0.