CEO CFO

ceocfointerviews.com
All rights reserved!
Issue: December 15, 2014
The Most Powerful Name in Corporate News

Watchful
Keep IT secret.

Data-Centric Security Solutions

***Charles Foley** – CEO*

Watchful Software
www.WatchfulSoftware.com

CEOCFO: ***Mr. Foley, what is the basic concept behind Watchful Software?***
Mr. Foley: I think the basic concept is that information security has become part of the public consciousness these days, and we have all realized that over the last 20 or 30 years we still have not figured out how to do it really well. We as an industry have approached it from a network perspective trying to secure the network or harden the perimeter against invading attackers who might steal the data. What is being realized is that some of the biggest breaches and most costly events take place when our own people, insiders who live inside the network, do things that are either honest mistakes, foolish acts, or even malicious actions, which was the case with Edward Snowden, Bradley Manning of WikiLeaks fame, and others. The fundamental basis of the Watchful approach is to put technology in place that will automatically identify sensitive and confidential information, literally at the moment it is created, whether it is emails, documents, spreadsheet reports, presentations or et cetera. Once that information is identified as sensitive according to the company's policies, it will be classified it into the right level of sensitivity, be it internal use only, confidential, secret or top secret. The information will then be marked and tagged, including watermarks, headers, footers, legal disclaimers, as well as getting a digital fingerprint on the information so you can see exactly everything that anyone has ever done with it. That includes every time it has been read, forwarded, printed, saved, exported or attached to an email, for example. Further, if the policy calls for it, the technology will encrypt that information so that the only people who can ever open it are people with pre-approved clearance by the organization. It doesn't matter if you have it on a USB key or if it is in a shared DropBox that you have access to, or even if someone steals your laptop and gets at the hard drive. Each individual item, each file and message, is individually encrypted and will only open if someone has the right credentials issued by the company. This is indicative of the shift from network-centric security to data-centric security that we see sweeping the industry. In a nutshell, that is our approach.

CEOCFO: ***It seems that no matter how strong someone's security is, there is always a bad guy out there that finds a way around it. Why are you confident that what you have developed will prevent any kind of slip up?***
Mr. Foley: I tend to agree with you - there is no such thing as an absolute answer. One of the thing you learned as a gunslinger in the old west is that there is always somebody faster. At Watchful, we are not saying that we are always going to stop the most vicious, well-armed, well-trained nation-state attack on your little business. What we are saying is that if you use our data-centric technology to identify sensitive information, classify it, mark and tag it, then encrypt it, you will be protected against the overwhelming majority of situations where data leaks out. If you look at the studies, the most dangerous and costly threats are insider threats where people do something foolish or malicious. Someone sends out the employee list to someone, and it includes their personally identifiable information and they did not realize that. Or, it might be that someone makes an honest mistake, such as the CEO of a company who types an email to the senior management team about a pending headcount reduction, thinking he is sending it to the 10 or 15 people on his senior management team, and doesn't realize until one second after he hits the 'Enter' key that the last name he typed was actually someone outside the company. That happens all the time.

If that information - at the moment it is created such as when an email is written, or a report is drafted, or when a spreadsheet is constructed - if it is automatically identified as sensitive and marked, tagged and encrypted…even if it does slip in the wrong hands by accident, you are protected. What if it is malicious in nature? Let's say you have a VP of Sales that is considering leaving the company. He is probably going to do what any VP of Sales does before he leaves a company…he is going to fill up every USB key he can get his hands on with customer lists, pricing, proposals, employee information and market demographics, etc. - and when he walks out the door your best information walks out the door with him. If, however, you are using our technology, he could load up dozens of USB keys and fill up his DropBox with data…but the moment you revoke his credentials that classified information will no longer open for him.

I am not sure that our industry has developed the 'one hundred percent solution' yet, because people can still do things like take pictures of screens with iPhones, or they can sit there with a pencil and paper and write down and memorize all the confidential information available. We cannot stop that, but what we can do is to get rid of the overwhelming 99+ percent of the situations that would affect a normal enterprise and protect them against the multitude of errors, foolish mistakes, and the overall majority of the malicious breaches that they face. That is really what we are targeting for.

CEOCFO: ***Who is using Watchful today?***
Mr. Foley: We have been really fortunate. We have customers around the globe, in key verticals including finance (since it is such a heavily regulated environment), telecommunications, and energy. Most people don't know this, but the energy sector is the second largest spending vertical in cyber security behind aerospace…they are paranoid. We have also had great traction in health care because of the PII, HIPAA and other compliance regulations. Government, technology, and defense are all very good strong areas for us. I think we fit very well for literally any enterprise that has sensitive and confidential data that should not get out, but we are getting our strongest traction in those organizations that face regulatory and compliance restrictions. If you look in the United States, for example, you have Obama's executive order on cyber security which came out last year, as well as the recent NIST cyber security framework, which for many people is expected to become a legal standard for duty of care regarding cyber information. If you look in Europe you have the new EU Data Protection Initiative that has been put in place, which has very firm monetary and legal implications if you have a breach. I think you will find that players in regulated industries are all scrambling to find the absolute best way to keep things inside the organization that need to stay inside the organization, and that is giving us great traction.

"I think what we are offering is the first time that there has been a streamlined, integrated approach that can have your information identified, classified, marked and tagged and encrypted in such a way that it is totally safe, but does not bother your users with additional effort or frustration." - Charles Foley

CEOCFO: ***What is the competitive landscape? Are there many companies attempting this approach?***
Mr. Foley: I think we are seeing a big shift in the market lately. The traditional approach over the last 20 years had been a very network-centric approach, but in the last five to seven years, you have seen a real increase in spending around data-centric solutions such as DLP (data leak prevention) initiatives. It was kind of a first wave, first generation approach from some very respectable companies like Symantec, McAfee, Web Sense and RSA; that approach was to keep data from moving from place to place where it shouldn't. The philosophy was, "let's block domains, block drives and devices, and let's keep data from being sent to a certain email address." That attempt to prevent movement is one approach, but it has proven to be pretty difficult because it requires stopping the movement of data – and with today's borderless environment of BYOD and cloud, you almost cannot stop the movement of data. It is the right thought process, however, to concentrate on the data as opposed to the network, so you see companies like Microsoft and ourselves paying much more attention now to the data layer.

You ask about the competitive landscape, and I think most of our customers feel that we have a good couple of years' head start in this streamlined, data-centric approach. Our ability to dynamically identify and classify sensitive information according to a company's policy - without the user having to do anything - places us really far ahead. The fact that what we are essentially zero friction at the user level, that we seamlessly enable the organization's security policy, and that we protect the vast majority of a company's data makes us valuable to our customers. That is what puts us at the forefront of the industry, but it is more than just that. It is also the fact that we embrace not only systems that are in the corporate network, like the corporate workstations, but we extend this paradigm of classification, encryption and protection schema all the way out to the billions of BYOD devices that you commonly see in the enterprise, such as Android, iPhone, iPad, and Blackberry devices…that makes us wildly unique.

Finally, our approach embodies the fact that not only that you need to protect your data, but if something goes wrong, you need to know exactly what went wrong and when. A great case for this is the European Data Protection Initiative regulation which specifies that if you have a breach, you need to define and disclose that breach within 24 hours. If you do not, that becomes the second offense, carrying a second penalty of up to one million Euro or two percent of your corporate revenue. Our centralized database, forensics and tracking means that our customers can literally tell you everything that happened to a classified piece of information. They can tell you not only who read classified information, but who printed it, forwarded it, exported it, or who saved it on a given storage device. That level of deep forensics makes us really unique. So, while I think there is some competition today, I think the industry is really paying a lot of attention to the data-centric approach and will continue to value our leadership position. I am not naïve, though, and I believe you are going to see, over the next five years, massive amounts invested in the space. Right now, I feel pretty comfortable that we have a good lead though.

CEOCFO: ***How does a company decide what level of encryption? Do you provide guidance?***
Mr. Foley: First of all, it's really each company's responsibility to decide and define what works for them. If need be, however, we are often able to help companies with insight on what constitutes a good information control policy. Because we get to work with some of the best companies in the world, we have a good handle on best practices around information control policies, classification, protection schemes, and we are certainly willing to share what seems to be the best practices approach for data-centric protection.

The specific approach, however, really is up to that company. I can line up 100 Fortune 1,000 companies and ask them if they have an information control policy and a defined taxonomy as to what types of information fall into what level of sensitivity…almost all of them will answer positively. When you go further and ask them if they have certain characteristics that are required of the information that falls into a given category, such as what level PII falls into or if it needs certain legal disclaimers, headers, footers or watermarks, they have very clear guidelines. Where it falls apart is when you ask them if they have any way to enforce that philosophy. That's where we step in.

It really is up to the company to define their policy, to define the levels of sensitivity and what makes information fall into each level of sensitivity, and how each level is handled. Most often, they already have the policy and the confidentiality levels, and they just never had a way to automate or enforce the policy before. That is what we present to them, and I think it is one of the reasons why we have been welcomed with open arms by most of the companies that see our product. It is our job to give them the technology that lets information protection happen automatically.

CEOCFO: ***Do you foresee a time when insurance companies would require this level of security?***
Mr. Foley: Not only do I agree, I do not think it is too far off…I think you are reading the tea leaves pretty well. You may know that in February of last year President Obama issued his Executive Order 13636, which basically says that you must follow a framework to ensure cyber security. He directed that to either government or commercial enterprises that deal with what is called 'critical infrastructure', which was broadly defined to include private enterprises where a cyber attack could jeopardize the economy or standard of living in a given area. If you are a major retailer, consider what happened with Target and Home Depot – a defined economic impact. It's increasingly accepted that companies such as this must have a framework for cyber security, and they have to follow industry best practices.

Furthermore, the executive order indicates that you should be in alignment with international regulations. Clearly, the EU Data Protection Initiative, which has mandated penalties of one million pound or two percent of revenues for a breach, illustrates where the international community is headed. In addition, under that initiative, if you do not identify and disclose that breach in 24 hours, that constitutes a second offense, which also carries the same economic penalty. Even further, the breach and failure to disclose can pierce the corporate veil to go through the corporation's directors and officers.

I think what you are seeing is that there is a lot of legislation saying that you need to consider proven industry-accepted best practices, and you need to follow defined frameworks. In February of this year in the United States, NIST, the National Institute of Science and Technology, came out with its cyber security framework initiative that is also expected to evolve over time. Right now, the approach appears that you must have a framework, consistent with best practices, and you must follow your cyber security plan. It would not surprise me if, a couple of years from now, you see strong guidance that directs inclusion of data classification, data encryption, et cetera as part of your plan.

So, I think you are reading the tea leaves, and I do think the government not only is going to get involved, but I do think the new data protection initiatives, executive orders, and outlined framework indicate a very clear trend that they are getting more involved, and that governments are very willing to tie very real financial and judicial penalties to those who do not comply. And that is when insurance companies get nervous.

CEOCFO: ***Do you see government as a potential area of growth?***
Mr. Foley: Most of our efforts to this point have been in the commercial business sector, as piercing the government market is very difficult, and it takes a lot of time, resources and investment. We are starting to allocate resources in the government sector, however, because I do see great opportunity there. Governments around the world, in particular the US government and the UK government, are magnificent opportunities for people that do what we do.

Consider the example of the UK government, where they have a government mandate on data classification. For years, it was known as the GPMS, the government protective marketing system. It stated that information of certain types had to fall into one of five levels of information sensitivity. They have recently refined that and brought it down to three levels of sensitivity, in the form of the GCS, or Government Classification System. You are faced with that requirement if you are a government agency, even a municipality, or if you are a major contractor working with the government. Information of certain types has to be classified, marked and labeled. That is a process that is almost impossible to do manually. Imagine the difficulty: if you have 10,000 users in your organization, how many of them really know what the policy is? How many of them know how to apply a watermark or how to put a legal disclaimer as a footer even if they knew the language that should go there? Imagine if all of that was done automatically, when certain triggers were tripped. That is what we bring to the equation.

I think the government is a great market for us, and you will see us expand pretty significantly there as we go through 2015 and 2016.

CEOCFO: ***It seems hard to resist you offering! When you are speaking with a potential customer, do they understand immediately or is there some skepticism?***
Mr. Foley: I find less skepticism than normal with new technology offerings. What I find most often is people saying they wish they would have seen this a year ago, when they were doing their budget!

When we show the technology, such as when we presented at Cyber Security Finance Forum recently and people see it in action, lights go off in their head. I get visceral reactions from customers who say this is the way it information security supposed to be done, and they ask why it has not been done like this before. There are reasons, technologically, because it would be very difficult if not impossible to do this 10 years ago with the technology available. However, technology has evolved, and we are going to take advantage of that.

With our strong initial response, we are now dealing with a lot of customers working through the adoption phase of our technology, and this is where they really love us. Normally it’s a difficult task to take a technology that the CISO knows and get it in place for 20,000 or 50,000 or 100,000 users. Our systems allows you to take a more gentle approach, where information is automatically classified for users but it does not keep them from doing anything in their job and does not change a thing about their daily life. Over time, about six months or a year, CIOs can start ratcheting up the levels of encryption or restriction actions that can be performed on classified information such as forwarding it or printing, until they evolve to a highly secured organization.

The fact is, most companies have been exposed and probably have been ‘bitten’. Ninety-percent of CIOs and CSOs surveyed last year said they had a breach of sensitive or confidential information over the prior twelve months. It’s a bleeding-from-the-neck problem. Once you see a way to easily address this without user revolt, that can be an evolutionary process, customers get more excited and less skeptical.

CEOCFO: ***Why choose Watchful Software? Why now?***
Mr. Foley: I think that right now information security is part of the public zeitgeist. It is a boardroom discussion, and every executive and employee understands that need. You need only look at what is happening after Bradley Manning, Edward Snowden, Target and Home Depot, and anyone can see that the need is clearly there.

I think what we are offering is the first time that there has been a streamlined, integrated approach that can have your information identified, classified, marked and tagged and encrypted in such a way that it is totally safe, but does not bother your users with additional effort or frustration. It gives you the levels of control that up until this point have been the domain of only exclusive large corporations and government agencies.

A lot of science over the last few years has gone into determining that the average cost of an insider breach of information is $1.035 million. If you add up the fact that 90 percent of organizations have been breached in the last year and everybody knows it and it has become a board-level topic, and that the average breach costs you one million dollars and if you do not do something different, the same is going to continue to happen again. You have heard it before – what is the definition of insanity? Doing the same thing over and over again and expecting different results.

We are a different approach, which is proven to give results. Why Watchful and why now? Because it works at zero friction, and you can begin to protect yourself today. Why now? Because most organizations do not have millions of dollars to continue to throw down the black hole of data breach liability and competitive disadvantage.

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

Contact: Rui Biscaia +351 918 684 313 rui.biscaia@watchfulsoftware.com