ceocfointerviews.com
All rights reserved!
Issue: June 1, 2015
The Most Powerful Name in Corporate News

SaaS Risk Management Solutions for Information Security And Compliance Challenges

Barry Kouns
President & CEO

CEOCFO: ***Mr. Kouns, your Risk Based Security website indicates, "Not just security, but the right security." How so?***
Mr. Kouns: We believe that there is such a tremendous threat environment to most organizations that they really do not know how to spend their limited budget. We have, in addition to consulting services, threat intelligence data that comes from both data breach information, that we have been collecting for the last 10+ years, and software vulnerability information. With those two data sets, we are able to help organizations figure out where their highest risks are and their most probable threats. With that, we are able to help them implement the right security, not just any security that some consultant may be trying to sell them.

CEOCFO: ***As security threats seem to change constantly, how do you get a good enough feel with the historical data to create a good plan or good recommendation for a client?***
Mr. Kouns: Great question, there is a new data breach publicized nearly every day. Last year, we had well over 3,000 publically disclosed data breaches added to our now database of over 15,000. I think it is common knowledge that there are numerous data breaches that are never published for various reasons, whether it is no regulatory requirements to do so, or companies just being fearful of making a breach public. As a security professional you can only react to the information that you have, and we pride ourselves on having the most comprehensive and timely information on data breaches, including how it happened, where it happen, who it happened to, what was exposed and how many individuals were impacted. In addition to our data breach information we are tracking over 119,000 software vulnerabilities, and like data breaches software vulnerabilities are being identified at a rate of about 1,100 vulnerabilities each month.

Every hour every day, we are tracking, validating, verifying and adding new software vulnerabilities to our database. Is it perfect data? Can we make exact predictions about what will happen next? No. However, if you are in the business of protecting sensitive information or developing secure software, or supporting an organization that is, you need access to the most complete data set available. This is the threat intelligence we provide to our clients and use it as a foundation for our security consulting business in helping clients identify where to spend their limited security dollars based on how the data relates to their business.

CEOCFO: ***Why can't we fix more of the vulnerabilities or not create them?***
Mr. Kouns: In business, there are generally three different pressures. The pressure of cost reduction and profitability, the pressure of product delivery, and then there is the pressure of quality or security. What we find is that most developers are incentivized to deliver quickly and inexpensively, and not so much on the security of the software. There are companies that take a very strong approach to security, and our data highlights which ones, but in the most part, developers make money by delivering new software and providing upgrades to software quickly and inexpensively. This approach to doing business is not new. The battle between cost, quality and schedule has been around a long time and right now, for many companies, cost and schedule are winning out over security.

CEOCFO: ***What are you providing to your clients?***
Mr. Kouns: We are providing a number of different products and services. We have the threat intelligence data we talked about earlier and many of our clients like to have access to the data via our SaaS Portal for research and alerting, and others like the raw data, so we sell subscriptions to both.

We also provide to full scope of information security consulting services, including information security risk assessments, network vulnerability assessments, security program development, SDLC expertise, and ISO/IEC 27001:2013 pre-certification consulting.

Perhaps our most unique service is what we call "YourCISO". A service built with the small to medium business in mind with little or no full-time security staff, but need access to security expertise. YourCISO is basically a virtual CISO offering where we provide access to our website that has basic information security and planning documents, incident response training and templates, security awareness training presentations, data breach intelligence reports, and through that portal they can contact us for a consultation or subscribe for a certain amount of support hours.

CEOCFO: ***Was it creating the technology to assess and assign risk with an algorithm? Is it the human input in the analysis? How do you weigh the different threats against the size of the company?***
Mr. Kouns: Everyone out there wants it to be pure math and science and pure data but, unfortunately, the data set is not complete. It is not like actuarial data when it comes to life expectancies for insurance or even the data associated with fire and general liability insurance, for instance. Everyone wants to know what the risk is in terms of dollars that a potential data breach or software vulnerability could lead to a data breach. What is it really going to cost?

That data set is very incomplete. It is incomplete in that those organizations that are breached are very stingy with the data that they release. Even if they release the fact that they have been breached, they are very careful about how it actually happened and what it really costs them in order to respond and recover.

"Risk Based Security equips organizations with security intelligence, risk management, vulnerability research and affordable on-demand security expertise through innovative, action enabling, predictive, and evidence based risk management solutions." - Barry Kouns

Everyone who looks at our data would love for it to be just a math and science exercise, but there is individual judgment relative to industry, size of company, types of data that you have, and how it may in fact relate or not relate to the types of data that has already been breached. It is also the science of trying to guess whether the data you have is of value to those malicious characters who want to get it. If you have financial information, social security card information or credit card information, you know you are higher on the target list. Some companies think that they do not have anything of value, which of course is not correct because most companies have employee confidential information at the very minimum and perhaps intellectual property. It is a combination of experience, trying to learn and see the trends that are occurring from both vulnerabilities that are being exploited, and the publicly reported breaches, then trying to figure out where your company may reside in that threat matrix, and then spending your money in the most appropriate, most valuable way possible.

CEOCFO: ***What might you look at when you are making that assessment that others would not add in the mix?***
Mr. Kouns: First, because we have 10+ years of historical data that is updated hourly, we have a sense of what might be coming down the road. We would love to be in a position to precisely forecast what is going to happen and when, and we are working diligently to transform our data, along with other data points into a more predictive model. For instance, our data would show that a particular software or a particular software developer has higher or lower levels of vulnerabilities in their products. Have they been improving or not improving over the years? What is their trend?

Our data gives you some insight into product procurement, in that if you are going to buy software, who should I buy it from? If I have a choice of providing companies, I might look at the data and determine which one seems to be producing fewer vulnerabilities than perhaps another. You can research data breaches and you can look at the actual types of data being targeted, such as credit cards, email addresses, user names, and passwords. You can then assess whether or not that data risk is one you need to address.

CEOCFO: ***Who is turning to you for services and who should be?***
Mr. Kouns: If you have valuable information, which if exposed could create extreme harm to your organization; you need access to our products and services.
Financial institutions, banks, credit unions, insurance companies, healthcare organizations and brokers for example, have a treasure trove of personally identifiable information along with account numbers that can be exposed by insiders and the malicious outsiders. Not only do these companies have what everybody is looking to get their hands on, but also the regulations have severe penalties if in fact they are not implementing good security practices.

In addition, any organization that is developing software most likely use software libraries. Third party libraries are pre-built pieces of software that many companies use to develop a larger program or solution. Because they are often open source, they can often be out-of-date and full of vulnerabilities. If you are a company developing software using some of these libraries, you need to know what vulnerabilities already exist in them so that you can make the appropriate decision of whether or not to use it, or to make sure that those vulnerabilities are repaired before they become part of your software.

Almost any large enterprise and need to evaluate potential suppliers or perform vendor management, you would want to know the security posture as best you could, and our data breach information helps you to zero in and protect yourself from exploits that start at your suppliers.

CEOCFO: ***How are you raising awareness so that companies know about Risk Based Security and understand they should be looking for more than just what solution they can throw at the problem to show that they are covered or to feel that they are covered?***
Mr. Kouns: Quite honestly, most companies have few alternatives without the threat intelligence data to guide them. Building a security strategy that is fact based, and not just opinion based on the last security vendor that just called them, they need access to real data, data like ours.

Our data allows a chief security officer to build a real strategy based on risks associated with their company using the fact-based data that we have been talking about – data breach and vulnerabilities – and a plan that could help form future budgets and explain to the board or CEO exactly why they are doing what.

The way we have been getting the word out is by attending conferences and being on the presenter list, meaning speaking at these various conferences, whether it be RSA, InfoSec World, the FIRST conference and many others. We are getting in front of the security providers and enterprises in trying to let them know there is data available to help them figure out a better way of protecting their companies and building more secure software.

CEOCFO: ***Do you find that people understand easily?***
Mr. Kouns: The security industry has often used Fear, Uncertainty and Doubt, or FUD. Generally causing people to be fearful and uncertain and doubt whether they are doing the right things to protect their information. That is generally effective, but we believe we need to educate and train companies on what they should be doing according to best practice and to provide the threat intelligence data to support any need to be fearful.

We find that when companies are faced with the threat data that is most relevant to them they are more open to help to build out a security program that is fact-based. In the security world, you never really want to be completely fearless.

CEOCFO: ***How is business?***
Mr. Kouns: Information security expertise is in high demand at present. All the data breaches, which you have probably seen in the news, give our business a real boost. The board of directors is starting to ask security people questions, and that generally means they get budget. When they get budget, they start looking for the best ways to spend it, and we are trying to guide them in ways to spend that budget.

Sometimes, how we guide them does not benefit us that much in that not all of them are ready for the products and services we offer. What we have done, and we are getting a lot of interest from small to medium-sized organizations, is our Your CISO as I explained earlier.

There is nothing more motivating than a data breach or a near breach to scare the board, the CEO or the owners of the company and there are plenty of those at present.

Enterprises are using our data for vendor due diligence and performance management. Another opportunity is emerging from insurance companies providing cyber liability insurance. You can imagine they would want to know all there is to know about a potential policyholder before writing a policy. Questions like, Have they been already breached? What kind of data do they have? What level of risk do they represent based on industry? Many insurance companies are subscribing to our data in order to put them in a better risk position to offer policies, calculate premiums and assess portfolio risk.

CEOCFO: ***Put it all together, why choose Risk Based Security?***
Mr. Kouns: First, I want to thank you for the thoughtful questions. It has been a pleasure talking with you.

Risk Based Security equips organizations with security intelligence, risk management, vulnerability research and affordable on-demand security expertise through innovative, action enabling, predictive, and evidence based risk management solutions.

Organizations are choosing Risk Based Security because of the powerful combination of our comprehensive threat intelligence with our practical expertise in putting the data to work. For companies with mature security teams, we help those teams be more effective by providing access to the best and most comprehensive vulnerability and breach intelligence available. That means time and resources can be spent addressing the most relevant security risks based on the very specific profile of the company. For others that need unbiased, straight-forward help with their security program, we back up our data with practical solutions designed to help leadership teams make informed decisions about how to best protect their company from cyber threats.

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

---

Risk Based Security

For more information visit:
www.riskbasedsecurity.com

Contact:
Barry Kouns
855-727-7475
barry@riskbasedsecurity.com