CEO CFO

ASTECH consulting

Issue:
February 24, 2014

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

Boutique Consulting for Internet Application Security

Business services
Cyber Security Consulting

AsTech Consulting
71 Stevenson Street, Suite 1425
San Francisco, CA 94105
415.291.9911
www.astechconsulting.com

Greg Reber
CEO

BIO:
Greg Reber is the CEO of AsTech Consulting and was among the first to recognize and address the risks presented by Internet websites.

Greg launched AsTech Consulting in 1997. Since then, he has established AsTech as one of the leading firms that financial services companies, retail service providers and other industries turn to for real world, effective information security solutions.

About AsTech Consulting:
Since its founding in 1997, AsTech Consulting has been helping companies meet the challenge of securing their vital information assets. Soon after inception, we recognized that the growth of e-commerce and the prevalence of web applications had fundamentally shifted the nature of business, and this was driving the need for new approaches to information security. In 2001 AsTech security engineers performed what might have been the very first source code security assessment for a major financial institution.

Since then, AsTech has built on that experience to offer a full suite of services related to application security. The company's mission is to enhance the capability maturity of our clients, by introducing proven best practices, processes, tools, and relevant metrics into every phase of a Secure Development Lifecycle. AsTech is known for its experts working with clients to find highly effective, cost-efficient solutions designed to maximize Return On Security Investment.

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: Mr. Reber, what is AsTech Consulting?
Mr. Reber: AsTech Consulting is a twenty five person boutique consulting firm focused on Internet application security.

CEOCFO: What is different about focusing on application security?
Mr. Reber: In the realm of cyber security there are two main categories; one being perimeter security. That would be firewalls and Intrusion Detection systems and the like. Then there is web application security, meaning the websites themselves which are actually computer programs that are made up of millions of lines of computer code, in some cases. That is where we focus, not the firewall or router hardware; but the actual software that is behind the websites that people use to do business on the Internet.

CEOCFO: What do you understand about the process that perhaps other companies do not?
Mr. Reber: There are three main parts; vulnerability discovery, that is the assessment, then prioritizing those results based on risk and planning some sort of action and then lastly, taking that action. What we understand, we believe, better than anyone is the second piece, prioritization. There are about ten companies in the world that very good at finding all of the vulnerabilities that may exist in a computer program. There is a *very* small number of companies who know what to do next, that is prioritizing the usually long list of vulnerabilities based on the risk they present, and creating the action plan to address them. Companies need to know that not all vulnerabilities present the same risk. A subset of the total vulnerabilities should be addressed immediately, because they present high risk. The next tier of vulnerabilities, based on risk, may be fixed in the next software release cycle, usually at about three months. The majority of vulnerabilities can be mitigated using existing controls, or devices can be introduced to mitigate the risks to an acceptable level. Every vulnerability in a website or Internet application does not present the same risk to an organization. We help people improve their understanding of these risks and prioritize mitigation efforts for the best ROSI – Return On Security Investment.

CEOCFO: What goes in to the decision of what falls into the different categories?

Mr. Reber: It really starts with the customers risk appetite. As long as people understand the risk that is present then they make a more educated decision, either accepting the risk or not. Therefore, what goes into that criticality rating, so to speak, is what information is at risk, and how easy is it to exploit some vulnerability? Is it customer records? Is it bank account information? Is it information that would be viewed as a target for intellectual property theft? We have to really understand what assets are being protected and how easy it is for an attacker to exploit the vulnerability. Those are the two main factors that go into a risk rating of some vulnerability that may be present.

CEOCFO: Are there particular types of companies or industries that tend to work with you, that understand what you can bring to the table?

Mr. Reber: Yes, financial services; banking in particular. That includes, stock trading platforms and trading companies. They are a bit more regulated and have been for longer periods of time than other industries. The financial services industry seems to get it more than other industries as a whole, but that is changing. Other industries are getting more and more on board with the importance of this area of risk management.

CEOCFO: Will you be looking to actively engage in additional industries or will that be opportunistic as it develops?

Mr. Reber: We are engaging more and more in healthcare, because there is increasing awareness there also. One of the aspects of client qualification is that if someone does not really understand this problem then they will not understand the value that a company like AsTech brings. Therefore, it really takes some level of awareness for a client company to be in our target market.

CEOCFO: When you are speaking with a company that is a prospect for your services is there a point where they understand? Where is the point where you realize that they are not going to get it and you should just move on?

Mr. Reber: An easy kind of litmus for that is if a company or a person responsible for the security of an application tells us that an automated scan of an application is all they need, because that will find all the vulnerabilities that may be present, then we know that they do not understand the problem. That's because there are very simple security vulnerabilities that an automated scanner will not find. With any automation it takes a human brain to start triangulating what the results actually mean.

CEOCFO: It does seem logical, just off the top of my head, to know that and understand that!

"Every vulnerability in a website or Internet application does not present the same risk to an organization. We help people improve their understanding of these risks and prioritize mitigation efforts for the best ROSI – Return On Security Investment." – Greg Reber

Mr. Reber: Yes it would! However, many folks who are responsible for all the security of their company and have to decide where to put scarce resources. Sometimes when it comes to application security the easy answer is "I have a hardware device for that, so we are good." To them that is a simple solution. There is a very good case in point. About a year and a half ago, a security hardware company had one their own firewalls in place protecting their network and it was down for maintenance and immediately; and I mean within minutes, got breached through a very well known application vulnerability called SQL Injection. Therefore, the devices are only effective as long as they are up and work only as well as they are configured, which is another complicated issue.

CEOCFO: AsTech Consulting has been around since 1997. Is that important to people these days or is it really more, what can you do for me now?

Mr. Reber: They are both important. Many folks are likely to say, "what can you do for me" and we can be right there with the best of them. However, when we say, "We have been in this business since 1997," then we get a bit more attention. Therefore, they are both important. Longevity does not mean that you are good. It just means that you have been around for a while.

CEOCFO: What has surprised you most as the company has grown and developed over the years?

Mr. Reber: What surprised me the most is that not everyone on the planet is beating our door down, since everyone who does business on the internet is at some level of risk. There are hundreds of millions of websites in the world. There are about two million websites that use SSL, Secure Socket Layer. That means they have something to protect and all of those two millions are not standing up risk management programs. Therefore, what surprises me is that this has not gained some sort of critical mass yet. However, I believe it is happening now, because once something is known it cannot be unknown. More and more people are realizing that, "Hey, we are at risk here! What are we going to do about it?" We are seeing much more awareness now.

CEOCFO: How do you reach out to potential customers? How do they find you if they are looking?

Mr. Reber: Referrals, thought leadership forums and word of mouth. When people leave one company for another, many times we will get brought in to their new company. We have a few clients who have programs in place where they will not buy a web application without it going through some security assessment process and we have an approved vulnerability assessment and prioritization process with a number of large companies. We have very good partnerships with some of the market leaders in the application security industry like Whitehat Security and Imperva that have brought business our way. In fact, right now I am at an application

security conference in New York and our Vice President of Application Security gave a technical presentation this morning. Therefore, we sponsor and we are presenting at the conferences for application security and many people are interested "who is doing what" that come to this conference. The conference this week is the largest in the world, by attendance. Traditional sales are difficult in what we do, because it is such a trusted position. There are some companies that we work for that have one main web application and if that goes away or it gets compromised by intellectual property theft their company goes away. Therefore, they have to really trust who they give their source code to for vulnerability discovery and remediation.

CEOCFO: What is your geographic reach? Are you working with companies' internationally?
Mr. Reber: Mostly in the US. The international work that we have done has been at the request of US based companies who are looking to buy software from a non-U.S. based company. Most of our engagements are in North America.

CEOCFO: Do you see that changing? Would you like to add an international component?
Mr. Reber: Yes.

CEOCFO: Are there any specific plans?
Mr. Reber: We will be established in Europe within a year. We're talking with some off-shore software development firms to partner with them on application security initiatives.

CEOCFO: Is it difficult to find and train people who can do that human analysis aspect that you talked about earlier?
Mr. Reber: Very! It is very difficult.

CEOCFO: Then, how do you?
Mr. Reber: We started the application security part of our offerings in 2001. What we found that worked best for us is to hire people who have at least eight years of enterprise application development on a large scale, not just small computer programs. We look for folks that who have been on product development teams and are looking for possibly something more. If they have done development and want to keep one foot in development, but want to do something else with that experience and are interested in security, then we bring them on. We have a very well thought out, well planned mentorship program. We pair them up with different individuals on various projects, so they get exposed to all of the ways that we discover vulnerabilities and remediate them. It takes about six months before someone can really stand on their own. The people that we hire and then train become very sought after.

CEOCFO: Do they tend to stay?
Mr. Reber: Actually, yes! We are hiring now. It is bringing down our average tenure down a bit, because we just hired two people. However, most of our team has been with us for at least five years, some more than ten.

CEOCFO: How is business today?
Mr. Reber: We had our best quarter ever in the third quarter of this year! The fourth quarter is looking very good and we have already booked up January and February, so 2014 is looking pretty bright.

CEOCFO: What is involved in an ongoing basis once you have a client?
Mr. Reber: For a typical security project, the first step is a baseline assessment on a web application, that could be anywhere from a mobile application with ten thousand lines of source code to very large web platform applications. Large meaning we have done assessments on applications that were four million lines of code. With a baseline assessment we look at everything that could possibly have a vulnerability and is part of the "attack surface" of the website. We report on these results, and then focus on the second step, which is to work with the client to prioritize actions. We try to help the developers who are responsible for the code fix the problems themselves, because that's the strongest and most robust remediation tact. Sometimes the clients want us to fix the problems and then tell them what we. However, we have found that there is a recidivism rate and more vulnerabilities may be re-introduced in later releases. Therefore, it is much better to "teach a man to fish" in this context, than to give him the fish. Then we come back on a periodic basis and to perform a differential assessment where we only look at the source code that has changed to make sure that no vulnerabilities have been re-introduced. In an optimal situation, this becomes part of the software release schedule.

CEOCFO: Why should people pay attention to AsTech Consulting?
Mr. Reber: We help keep their companies' future safe. There is the old adage that "you are always fighting the last war." That applies here. When you look at what the bad guys are doing, they do not rest and they are always looking for the next vulnerability to exploit. The ones that everyone is really concerned with; I do not want to name any countries, but Eastern European organized crime and some of Asian groups that are more interested in intellectual property theft; they are relentless! They will not stop and they know what they are doing. Therefore, it is an ongoing and ever-changing threat environment. What we at AsTech understand is staying on top of that threat environment is key for understanding and defending against any new vulnerabilities. We are always scanning and researching for new issues. We do some research on our own to try to come up with vulnerabilities before they hit the wire. One of the attributes that is somewhat unique to AsTech Consulting is that we have been able to optimize and refine our process over twelve years of hands on application security work, where some of the other folks that are in this space jumped in just in the last four years or so.

CEOCFO: Is that where the experience and longevity comes in?
Mr. Reber: Yes it does. Anyone doing business on the Internet has these risks. Just because they have not shown up yet in some ways may mean they are not measuring the right thing.

Also, as I said, the bad guys that everyone is worried about may get in, take what they want and get out without anyone knowing it. If there are vulnerabilities in the web application or the website they want to be able to keep coming back. Therefore, if they can hide under any kind of detection or through web applications, there are very easy ways to do that which many folks are not even looking for, so they will never know. Until they show up on the front page of the Wall Street Journal.

AsTech Consulting
71 Stevenson Street, Suite 1425
San Francisco, CA 94105
415.291.9911
www.astechconsulting.com