ceocfointerviews.com

Issue: May 18, 2015
The Most Powerful Name in Corporate News

Cybersecurity Analytics Platform for Global 2000 Organizations

Ray Rothrock
Chairman & CEO
RedSeal Inc

CEOCFO: *Mr. Rothrock, what is the concept behind RedSeal?*
Mr. Rothrock: RedSeal provides a cybersecurity analytics platform that executives can use to certify that their current networks are secure. So what does that mean? You, as a company executive, perhaps like many Wall Street firms, have probably invested significantly in security software. Yet every week we read about new security incidents or breaches. Even though people have implemented a lot of security software already, there are still vulnerabilities. That's where our product comes in. Our cyber analytics product ranks and rates all of that technology over your whole network—and not just your security products, but your network devices, as well. It then gives you metrics that tell you—on a business level—where the risks are, prioritizing them based upon where attackers can still gain access to sensitive parts of the networks. And this is monitored over time so as your network shifts to accommodate for business changes and growth, you can see where your network is exposed to new risk, and where it is, enabling your organization to take immediate and direct action.

CEOCFO: *What are you actually measuring?*
Mr. Rothrock: The first thing we do is model the network— all the firewalls, routers, load balancers, etc., anything that's routing traffic. In the routing world, for example, data often goes to places you wouldn't expect or cannot identify. That's a potential risk. The challenge is that without RedSeal, there's no way of seeing and understanding it all, and I assure you no one does. I have yet to see an organization run the software in a large enterprise and not come up with significant surprises. Also, there are a lot of computers and servers in your network. Let's say a large corporation has 50 Oracle databases… not all of them will be equally important; one may contain social security numbers, another may have just have a bunch of web pages used for advertising. The point is, these are very different assets and thus very different risks if that information were to be hijacked or stolen. We can determine, based on the content of each host, how important they are to your business. Important assets should not be connected to the outside world unless it's done properly. Another thing we measure is how the network changes over time. Networks are dynamic—they change every day (for example, firewall rules) and that also changes the level of risk. You want to have some assurance that your network is secure, and that level of security remains stable. As your security metrics improve, your risk score goes down. Those are all benefits that RedSeal provides, and there are a lot more.

CEOCFO: *What will a company see on a day to day basis to help make decisions, or are you making decisions for them and how they react?*
Mr. Rothrock: Our enterprise software solution is installed on a customer's server— they run and operate it. This will let them see changes to their network; for example, they will see when a division puts up a whole new network, or when a new subnet is turned on. And they'll understand whether changes like those have made their network more or less risky. Another example, using M&A (Mergers and Acquisitions), is this: Let's assume you're about to acquire a modest sized company. Wouldn't it be smart to run a cyber analytic risk analysis of that company's network *before* you attach it to yours? It's a little bit like a home inspection—you want to know if there are termites. Those are a couple of examples of how RedSeal can be used on a day-to-day basis.

CEOCFO: *What has people most surprised when you first start with them and they see the risk?*
Mr. Rothrock: Here's a typical scenario… The people who operate complex networks have documentation, diagrams and maps of their network. We use that information to start our analysis, and we can then calculate -- based on information that we get from the actual network -- not just what is off their paper, but what the actual routing table might be. We find

other devices that they didn't even know existed—hosts, routers, and unknown connections to the outside world that they didn't know about. That's a typical response and actually a very scary one. We had one large security company run our software, and in the process they shut off a number of connections, eliminated some network protocols that were no longer valid, and saved themselves millions of dollars in operational costs that quarter. With RedSeal, you learn what you didn't know. You know that old cliché— you don't know what you don't know. We can actually show you what you don't know, and prioritize problem areas; then you can take actions against that information or leave things the way they are. It's up to you, but now your choice is based upon true knowledge.

CEOCFO: ***Do you follow up to find out that they are not only paying attention, but are acting on the information?***
Mr. Rothrock: They *are* acting on the information. In this age of data breaches -- particularly since the Target attack in 2013 -- it's become a critical issue. Let's say we identify a risky part of their network that has got some assets or some information that would be bad if it leaked. If they don't take corrective action they are liable for the losses. That's bad business, but it's also become personal. The Target guys lost their jobs because they knew they had problems and did not make the right decisions. These networks are big and complicated. Companies don't have infinite resources—engineers or money or time. Therefore, you have to start with the most risky issue, and that's a core value that we deliver. We show what in your network you must really fix now. Then you can test it to see that you have it right, and then go to the next thing and the next thing. The risk score that we now calculate has been received very well. It used to be that the Chief Information Security Officer would go in to the CEO and say something like, "We have eliminated attacks," followed by a lot of technical details that the CEO wouldn't be able to follow. Executives are used to listening to hard numbers. With RedSeal, for example, we can say that yesterday we were at a 700 risk score and today we're at 650, and show them what changed. They don't have to understand all the technical details to know that they are either better or worse. We do that for the executive suite.

"The bad guys have to be lucky once, but we have to be lucky 100% of the time. RedSeal improves your odds of being right 100% of the time." - Ray Rothrock

CEOCFO: ***What types of companies or organizations tend to use your services?***
Mr. Rothrock: A typical customer has more than $100 million in revenue. They have large and complex networks, and usually geographically dispersed or global. All of the major verticals—technology, retail, financial, utilities, service providers, military and many US government agencies use our technology. In fact In-Q-Tel (IQT) is one of our investors, and is delighted with our results, because our software is being used on the front lines to continuously monitor some of the most critical networks to ensure they're not getting tampered with by the bad guys. I'm also proud to say that a number of the largest security vendors are among our customers, including Symantec, FireEye and Cisco. They use our software to help protect their own networks. These guys are big security players so it's exciting that they view RedSeal as essential for their own security.

CEOCFO: ***You have recently added to your team. What is changing for you? Why is this the time for a bigger push or a bigger footprint?***
Mr. Rothrock: One reason is the sheer number of breaches. Here's how I see it: The Target breach made everyone aware that networks are not perfect and the Sony breach last December scared everyone. That's making other companies step up their security and risk management game and really grasp it, understand it, measure it and then take remedial action. And networks are embedded deep within the strategy of companies. If they don't work properly, or parts of their businesses are at risk, that's not good. I like to use this fire sprinkler analysis: You build a big warehouse, put a bunch of inventory in it, but don't put any sprinklers in it…so what happens if the warehouse burns down? Your network is like that. It's enabling business and commerce, transmitting important information, conducting inventory measurements and so forth, and all of your information (HR, contracts, etc.) is flowing around on it. If the network breaks down, your business stops operating. A cyber incident can significantly hurt or even kill your business.

CEOCFO: ***Where does mobile come in to play?***
Mr. Rothrock: We include wireless routers in our network model. And, one of the new features that we've implemented is providing network visibility all the way to physical host connections, which are referred to as Layer 2 in the OSI stack. We used to providing visibility to Layer 3, which is how things are connected logically, and now we've extended that further.

CEOCFO: ***You went to school for nuclear engineering. What did you learn in that part of your education that has been helpful at RedSeal?***
Mr. Rothrock: That's a great question. When I was studying to become a nuclear engineer back in the 1970s, a process called "defense in depth" was introduced. It's about how to think beyond just a single element of a system—for example,

keeping radiation in—and takes into account how the entire system works. In that scenario, you would have the fuel rod, water, the vessel, the building and all, but these are just elements. How it all works together is the important element to the safety of it all, for instance, how the pumps turn on if you have a leak. I've been doing cyber security for 20 years. I was one of the original investors in Check Point and many other cutting-edge companies in the 1990s and the early 2000s. Thinking about network security from a big picture point of view, not just a specific feature or a firewall port or a specific virus, is very important. You need all that to implement security, sure, but how it all functions, as a system to protect the enterprise is what's really key. It's the same concept as designing and running a nuclear power plant.

CEOCFO: ***There are many companies in your industry. What sets RedSeal apart?***
Mr. Rothrock: Those companies all sell great products, and they all have a purpose. RedSeal does not eliminate the need to have a firewall or the need to have intrusion detection systems or anti-malware products. In fact, plenty of our customers have said that when they run our software, they see better ways to use those other security investments they've made, improve upon what they already have, or even to use less of it. We have customers that use RedSeal to plan their network expansions and their future "buys." The other products do very specific blocking and tackling, but you need RedSeal to understand the big picture- how it all works together. That's how we are different. Five years ago that was not interesting to very many people. RedSeal was a little company and we had few customers. However now, in this age of the data breach, people are beginning to appreciate that even though they may say, "I have the best firewall," or "I have the best APT detection capabilities," or "I have the best this and the best that," they want to know why they're still getting hacked and broken into. It's simply because they don't understand the entire picture of their networks. That's what RedSeal does, and it gives you metrics around how secure your business is.

CEOCFO: ***Final thoughts?***
Mr. Rothrock: It's a new age. Attackers are getting smarter. The bad guys only have to be lucky once, but we have to be lucky 100% of the time. RedSeal improves your odds of being right 100% of the time. We are very committed to helping companies eliminate that insidious tax called the cyberattack. It erodes business, and if we can stop it then everyone is better off. Our economy can grow faster. Our tax base gets larger. Right now, when I'm giving speeches, people ask, "Do you worry about a 'cyber' Pearl Harbor?" I say, "Yes, I worry about it, but I'll tell you what I worry about more… I worry about the attacks on every company, every day, and, in fact, every minute of the day." There are 10 million businesses in the United States that largely cannot defend themselves, and the government certainly can't defend ten million businesses. It's all about working together and sharing threat information and making people operate their networks better, smarter, and more effectively.

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

RedSeal Inc

For more information visit:
www.redseal.co

Contact:
Paula Dunne
+1 (408) 776-1400 o
+1 (408) 893-8750 m
paula@contosdunne.com