



With Cyber Attackers Still Penetrating the Most Sophisticated, Layered Defenses, CounterTack is Leading the Way in New Solutions for In-Progress Deeper Security Intelligence Monitoring and Faster Attack Response

**Business Services
Security**

**CounterTack
303 Wyman Street
Waltham, MA 02451-1208
855-893-5428
www.countertack.com**



**Neal Creighton
CEO**

BIO:

Creighton has more than a decade of experience in IT system security, identity verification and Web authentication markets. As co-founder, president and CEO of GeoTrust, Creighton was responsible for providing the leadership, strategic direction and management for the company. Creighton spearheaded GeoTrust strategically and positioned the company for rapid growth. Creighton led the efforts to raise \$24 million in venture financing and sold GeoTrust to

VeriSign (NASDAQ: VRSN) for \$125 million in September 2006. In addition, Creighton led the spin-off of ChosenSecurity from GeoTrust, which was acquired by PGP, Inc. (now Symantec). Creighton was also co-founder and executive chairman of AffirmTrust LLC, which was acquired by a Trend Micro in 2011, and co-founder of RatePoint, Inc., which was named MITX 2010 Social Media Company of the Year for New England.

Creighton is a graduate of the United States Military Academy at West Point and holds a Juris Doctorate and Master of Business Administration from Northwestern University. He is also the co-inventor of the domain control authentication patent granted in 2006 and was a Massachusetts High Tech All Star 2010, 40 Under 40 award in New England, three-time Ernst & Young Entrepreneur of the Year finalist and 2007 Sale Side Deal of the Year winner for New England from Mass High Tech.

About CounterTack:

CounterTack, the industry's first and only in-progress attack intelligence and response solution provider, was born out of the critical need to develop new security approaches for enterprise and government organizations. The detection gap persists despite massive investments and continuing advancements in security technologies, with cyber attacker innovations outpacing cyber defenses. CounterTack is leading the way on new approaches for deeper security intelligence monitoring and faster attack response.

The need for a completely new approach is clear. Each year, more than \$32 billion is spent worldwide on security technologies, yet motivated cyber attackers are still finding ways to penetrate the most sophisticated, layered defenses.

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

CEOCFO: Mr. Creighton, would you tell us about CounterTack?

Mr. Creighton: CounterTack is in information security. We offer network monitoring and attack detection intelligence and are aggressively working to close the detection gap. You cannot pick up the newspaper today without hearing about an organization that has been attacked, penetrated or hacked. Critical information is all too often falling out of organizations, from the New York Times to government agencies, even security companies like RSA Security. The motivation behind these attacks relates to the critical nature of information within these organizations, the U.S. economy and the defense industry. There are other countries, other people and other organizations – even criminal – that want to get their hands on that kind of material. The tools they use to attack are very advanced. Likewise, the security tools used to defend are a generation behind. And that's what creates the gap. CounterTack delivers new security technologies that can detect advanced attacks that other technologies cannot.

CEOCFO: What is the approach and what are the specifics about how you

accomplish what other security technologies cannot?

Mr. Creighton: Today, when an attacker goes after an organization, they usually send things called “malware” to the organization. Just like consumers have antivirus running on their machines, organizations have some type of technology running within their networks to detect these things. When these attacks happen, attackers take over machines and work their way through networks to grab critical information. It usually takes place over a long period of time; often times, hackers remain in a network for years. However, technologies developed early on to detect malware viruses were based on what we call “signatures” or known threats. In order to detect them, you would have had to see the malware or virus somewhere else and created a specific signature or a fingerprint to trigger a notification that you have seen that kind of threat before, prompting you to block it. The problem today is that we have a huge gap in what traditional technologies can detect versus what kinds of attacks are coming in. At any point in time, 50 percent or more of malware programs are getting through traditional security defenses, because they are not known threats. New attacks are specifically designed to breach an organization in ways that traditional defenses will not detect. Other attacks are evolved from known pieces of malware that have been changed, crypted or delivered in some other way that alters its appearance. Once attackers get in and get behind your defenses, they can do an awful lot of damage. We recognize, as an organization, that you cannot keep up by looking for known threats. You have to look at behaviors. There is a lot of commonality in the behaviors of malware that hit a machine. CounterTack’s researchers constantly monitor within the target environment – laptops, desktops and servers – in a variety of ways.

CEOCFO: Would you elaborate on the behaviors?

Mr. Creighton: When a piece of malware hits the machine, it is going to try and take over. To do that, it has to

manipulate your operating system. CounterTack looks for those manipulations from a very low level – our technology is like a camera watching all of the hackers’ movements on the operating system in real-time. As it sees known hacker behavior, it triggers a notification to say that attacker behavior is happening on this machine and therefore, it is now infected.

CEOCFO: Has this approach been tried before? How are you able to do it? Was the idea around and other security vendors were not able to implement it or is this a totally new way of looking at the security problem?

Mr. Creighton: CounterTack’s approach to attack detection is a completely new way of looking at the problem. Old techniques were not working. If you spoke to an organization three years ago and said, “You are going to be breached by a hacker, they are going to get past your defenses. You have to accept that,” they would have looked at you like you were crazy and replied, “No, I am not going to accept that, because I want to keep them out.” Today most organizations realize that they cannot keep attackers out. It is all about how quickly you can detect an attacker once they have gotten in. We have been preaching this and evangelizing it for a number of years. CounterTack designed its technology around this. There are certainly other companies attempting to enter the space, but CounterTack has a huge “first mover” advantage. The ability to observe an attacker and see what they are doing is not easy. It requires years of research and development (R & D), engineering work and a different mindset to create this technology. It is a new way of thinking about things, driven by the necessity of protecting information from attackers that are going to get in to your network. Information is still being stolen, you read about it every day in the newspaper. Organizations need to have a different approach. That is what CounterTack is: a completely different approach to dealing with an attacker.

CEOCFO: Do people “get it” right away? Do they understand the concept?

Mr. Creighton: Markets evolve very, very rapidly when there is an urgent problem to be solved. Two and a half years ago, the industry did not exactly “get it.” But everyone understands today that they likely have already been attacked, are probably currently under attack, or will soon be attacked. If you talk to a large company’s head of security and ask, “Do you know what is going on inside your network? Do you have good visibility to what is happening on your servers and workstations?” They will have to tell you “No.” They inherently “get it”. I predict we will soon see a dramatic shift in the security industry where larger companies that you have heard of in the past – Symantec, McAfee, Checkpoint and other folks who are focused on more traditional ap-

“The detection gap persists despite massive investments and continuing advancements in security technologies, with cyber attacker innovations outpacing cyber defenses. CounterTack is leading the way on new approaches for deeper security intelligence monitoring and faster attack response.”- Neal Creighton

proaches – will still be around, but new large security companies will emerge. Companies like CounterTack are already emerging with new and more effective technologies, which will position us as market leaders in the near future.

CEOCFO: You have an infinite market. Who are you approaching? How are you approaching them? What is your strategy to go from having this great product to getting it in use?

Mr. Creighton: The interesting thing here is that the pain is being felt pretty much everywhere. Just look at the attackers themselves. Who is attacking organizations? Why? We’ve found there are basically three groups. First are state-sponsored attacks that are coming at our commercial entities to steal intellectual property. They are coming after the government to steal secrets. There is an obvious benefit to that from their side,

which explains their motivation. There also are organized criminal elements coming after information for financial gain. It took us forever to get the Mafia under control and it is still not under control. When you look at criminal organizations across the world that work anonymously on the net, they are very hard to control. And then you have hacktivists, who are out there as the self-proclaimed Robin Hoods of the 21st century. Hacktivists are attacking large organizations, taking information and shutting them down. They are using new tools to do it and coming from all different directions. They are attacking pretty much everyone. However, if you look at who has the most to lose in terms of assets, you can understand why financial services organizations and banks are very heavily targeted. The government is also very heavily targeted. Really anyone who has intellectual property that their business depends on is getting attacked. CounterTack has focused on large Global 2000 companies in financial services, manufacturing and technology. Our sales team has been going after these organizations directly. CounterTack also has partners that are emerging for us and helping us get out there.

CEOCFO: Do you envision a time when it would be available to consumers?

Mr. Creighton: Yes. You are talking about our dream. When we describe older technologies, they are not really that old. Everything just moves fast in technology. You are probably running McAfee, Symantec, Trend Micro or something similar on your machine today. They are looking at known threats coming in, but CounterTack looks at the unknown; we are looking at behaviors to detect attackers. That kind of monitoring would be very useful to a consumer, because you can imagine that attackers are going after consumers for financial gain. As we continue to build our company and look a few years down the road, we would like to be able to offer this type of enterprise grade protection to an

individual consumer to keep their laptop or desktop safe; we'd be the next generation of antivirus or anti-malware.

CEOCFO: Is CounterTack funded for the foreseeable future?

Mr. Creighton: We are. We are a private company and go through the typical stages. Since I have been here we have put about thirteen and a half million dollars into the company from investors. Some of our investors include Fairhaven Capital, which is located here in Boston, and also a group of private investors. As you can imagine there is a lot of interest in this space and in CounterTack specifically. Funding will not be an issue for us, it is more important for us to move as quickly as we can and grow as much as possible before another company sprouts and tries to take the market away from us.

CEOCFO: Why should investors and people in the business community be paying attention to CounterTack?

Mr. Creighton: The world is changing. On a fundamental level we are all connected on the internet, and that's a very powerful thing. It is transforming the way we listen to music, how we bank, how we communicate as a business with our remote employees; you name it. It touches us at almost every moment of every day. There is a huge benefit to that, but also huge dangers to being so connected. It is becoming easier for hackers to reach people's assets and intellectual property: money and personal information. There is a lot of money to be made from criminal elements. There is a lot of opportunity for other countries to gain access to U.S. secrets and accelerate their own economy and R & D. We need to have robust security and recognize that hackers are persistent, very smart and very well organized. The technologies needed to defend ourselves have to be as advanced as the approaches attackers use to steal information.

CEOCFO: What have you learned from your previous ventures that have been most helpful for you here?

Mr. Creighton: That is a very good question. Persistence pays off. Being an entrepreneur, there are always ups and downs. You have to be very persistent in your beliefs. When you start a company, it does not always end up taking the path you originally planned it would; actually it almost never does. You have to be persistent and flexible when you build a company. Another key take away from my career learnings is that people have great ideas, but market timing can sometimes be off for those ideas. Some business plans sound rock solid, but if the market is not ready, your company could run out of financing or run out of time before anything comes to fruition. For example, with CounterTack, I came in from the outside when the market timing and technology lined up. It is a tough time. There are a lot of attacks happening every day, and we needed a new approach. I took one look at the company and knew that it was in the heart of the storm. This has been a critical lesson I've learned through previous attempts to build a company and make it successful. You have to survive to win and persistence is a big piece of that, and then there's the market timing, of course. We're in a very important time when it comes to how information is secured, because we are all globally connected. It is a dangerous time. As I said, you can pick up the newspaper every week and read about someone getting hacked. At the same time, I think it is a natural cycle – necessity drives innovation. I believe that we are going to solve this problem, until the next problem arises. We are on the verge of building companies that will truly protect critical information and private networks, and CounterTack is one of them. It is a really exciting time to be in security. There are great challenges in our field, but I believe very strongly that CounterTack is meeting those challenges.



CounterTack

**303 Wyman Street
Waltham, MA 02451-1208
855-893-5428
www.countertack.com**