ceocfointerviews.com

Issue: November 3, 2014
The Most Powerful Name in Corporate News

Online Security and Privacy Protection

David Lowenstein - CEO

About HACKJACKET
HACKJACKET provides everything you need to Protect Yourself online and personally control the security and privacy of your online data, content, communication and browsing. Powered by radically new threat immunization architectures, protocols and technologies, HACKJACKET seamlessly and comprehensively provides provably effective protection against networked software's most pervasive threat vectors while maintaining 'Zero Knowledge' of our user's data. Our current products include: the HACKJACKET Personal Internet Protection Suite and our CloudGate Internet Identity and Access Management crowd funding project. Founded in 2005, HACKJACKET is headquartered in Toronto (Canada), but we protect you and your data everywhere you go online.

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

CEOCFO: ***Mr. Lowenstein, what is the concept for HACKJACKET?***
Mr. Lowenstein: The basic concept of HACKJACKET is protecting yourself online and doing it in a way that we tagged as universally universal. Without just trying to be pithy, what we mean by that is that the one way we spell universal is "You", so what it really means is user centric, which means you should be able to control the security and privacy and everything you do online, because after all, it is your data. The second is this concept of universal, which is to protect everything that you do on every device against all attacks. That really was the concept of the company, HACKJACKET. The idea of the "HACKJACKET" was really a play on flak jacket, but instead of protecting a person and their vital organs; we are protecting your vital information offline. That was the genesis of the concept, the branding and naming of the company.

CEOCFO: ***What do you understand fundamentally about protection that others may not understand as well?***
Mr. Lowenstein: The first thing is we asked ourselves that very question nine years ago when we entered stealth mode, which is a long time but it is a hard problem. The "Copernican moment" for us was the realization of three things. One was pretty well every existing solution including up until present time, is on a model or take an approach that we call sterilization. What that means is they are trying to keep bad stuff off your computer or device. It is things like firewalls and antivirus, all about keeping bad stuff off something. If anything the last decade or so has taught all of us is that it is next to impossible to keep bad stuff off things whether it is a network or your device, they will get on. What is really required is more of a concept of immunization, so just like sterilization did not work for Howard Hughes, it really does not work in the online environment. That really was a big revelation, aha moment for us. We started working on set of technologies that were immunization oriented as opposed to sterilization oriented. When you sterilize anything such as medical equipment, you are trying to get all the germs off and keep the germs off. When you immunize something or someone, you are expecting that they are going into a germy environment and even if the germs come in contact with them, it will not matter. If you are immunizing someone, you could put them in a bubble to keep them away from a cold or flu or you could get a flu shot because you are going to come in contact with it, but when you do, the flu virus will not be able to impact you. In a more technical sense, the assumption that we made is that even if world class state actors like the people hired from the NSA were directly on your machine, they had direct access to

your machine, so how do we even protect you in that environment and if we are able to do that, you would affectively be immunized from hackers. That was the basic mental model and technology model that we started building towards.

CEOCFO: ***How do you do it?***
Mr. Lowenstein: You do it a couple of different ways but it really starts with some fundamental building blocks and some of these are very hard which has taken us a long time. The core thing that everyone us now doing is encryption. It is kind of the first item on the checklist and it is pretty simplistic. Most people do it, but not everyone does yet what we call a user centric encryption. That means that only the user has access to the keys. The keys are not with your service provider like Google or Facebook or whomever. Only you have the key and that is an important concept because it means that when the government or some other body comes calling saying they would like the data, even the service provider cannot provide it. All they can do is give them encrypted data. Generally people think encryption is pretty strong and that provides a great deal of protection. The first thing is to protect the data and I think pretty much everyone has come around to that point of view and not everyone is quite at the extent of personalized protection or encryption, but we think that is coming. The bigger and much harder thing is what we call protecting the data path and that is you need to protect that data everywhere it does. The basic idea is that nobody can read encrypted information. It needs to be transcribed to a human readable format. However, the second it is transcribed, if there is an attacker, they are simply going to wait for you to open it and the second you open it and read it, they are just going to go after the data when you read it. Therefore the second thing is protecting the data path. That is much more difficult and has to do with the interface of the user/computer/human interface to the operating system, to the application, so we have developed a series of technologies that do that. The other thing that we have done that is very important and different is we have protected and added enhancement to FSL secure socket layer, which is sort of the lock that you would sometimes see on your device that encrypts the communication between yourself and a service provider. It is generally good but it does have come significant flaws weaknesses and we have plugged all of those. That is another important leg on the stool of what we do. The critical thing is that we protect the data and everyone is starting to do that. The other is protecting the data path, which is much more difficult.

"The thing that gives us the confidence is, having taken a scientific and metrics oriented approach, which is security and privacy products need to stop attacks, full stop. That is your real purpose in life and if you cannot do that, you are not doing much and the bottom line is we stop more attacks than anything on the market today and we are confident that we pretty much solve everything that is currently out there in terms of known digital attack threat models." - David Lowenstein

CEOCFO: ***Is your product in use? Do you have a finished product yet?***
Mr. Lowenstein: Good question. In the development cycle, we are basically in final testing of what we call our personal product. We are currently only running on windows and developing the phone product as we speak. We have a server product as well that we call Cloud Protect. We are in the final testing of the personal product, probably about 80% dine on developing the cloud product and probably only 30% or 40% on the mobile product.

CEOCFO: ***What have you learned along the way? What has changed since you have been doing testing?***
Mr. Lowenstein: One of the really interesting things for us on our journey here in the last nine years of developing this product and testing it is that most of the attacks that everyone has been reading about in the paper, whether it is cyber criminals stealing credit cards from folks like JP Morgan, whether it is the NSA spying on their citizens, or whether it is government actors trying to use Chinese, Russian, American or otherwise, trying to usurp data for whatever purposes, there was a pretty good understanding and there has been for a long time around the potential scope of the attacks, but nobody had really seen them in the wild . They were least conjectured among a bunch of ivory tower types and not taken all that seriously. What has really transpired is we not only protect just the working of our product but really important to security and privacy that we provide our users is that the threat landscape even though it has not changed, it is has become much clearer that these attacks are very clear and present dangers, whereas before they were just concepts

and hearsay. I think the last 3, 4, 5 years in particular have brought all of that home that those previous conceptual attacks are now very real and that people need to be personally protected form not only bad guys out there in the nether, but also in terms of potentially protecting themselves from their own governments in some cases. It really has been a seat change in awareness and understanding of what is really possible, because the possible has become very probably now.

CEOCFO: ***What is your plan for the next year or so?***
Mr. Lowenstein: Our plan at this juncture is over the next probably 45-90 days we are going to start releasing our product probably in an alpha mode, so more of a technology release. We are thinking about with some of our more advanced solutions, doing a little crowd funding, which has become very popular. We have been self funded to date and we like the autonomy that brings. To take this company to the next level, it does need some financing. My business background has been both private and public in the public markets. I raised a great deal of money and I think there is some tremendous value in a public market environment. Certainly in the case of security and privacy products like ourselves, there is a real benefit to be private and autonomous. Even though we recognize the need to have more fuel in the tank to more things faster, now that we are past the R&D stage, we also recognize that we should try to maintain that autonomy, so we are thinking about crowd funding. In a short answer, looking to raise some capital; crowd funding or otherwise and start releasing our product suite of first and foremost, starting with a personal product on Windows and probably follow that up with a suite of cloud protection products, and then shortly after with mobile.

CEOCFO: ***What gives the confidence HACKJACKET has the answer?***
Mr. Lowenstein: What gives us the confidence is two things. One is the attacks that read in the paper are extremely well known, easy to replicate, and at the end of the day, security and privacy, although it is very complex, testing it is relatively simple. You either stop an attack or you do not. Everyone knows what the attacks are and in today's world. Nobody can stop them. The attacks that we are aware of both on the security side and the privacy side, we can stop. We have been testing that over the last nine years and we've continued to test as things develop and as new things come to the forefront from the realm of academic conjecture to reality. The NSA, Snowden revelations are a great example of that. We have back tested our solution for those very attacks and in some cases modified what we have done to be a little more robust, but in most cases just already stopped them out of the box. The thing that gives us the confidence is, having taken a scientific and metrics oriented approach, which is security and privacy products need to stop attacks, full stop. That is your real purpose in life and if you cannot do that, you are not doing much and the bottom line is we stop more attacks than anything on the market today and we are confident that we pretty much solve everything that is currently out there in terms of known digital attack threat models.

HACKJACKET

10 Four Seasons Place 10th Floor
Toronto, Ontario Canada
416-649-5751
www.hackjacket.com