

Encryption Solutions for Hard Drives, Media and Cloud Storage

About Data Locker

In an environment where many people are turning to USB external storage devices because of growing file sizes and larger amounts of data, protecting lost or stolen devices – and the information stored in them – is no longer a luxury. Using patented technology, DataLocker offers encryption solutions for hard drives, media, and cloud storage to provide peace of mind to today's workforce. Our products are lock-tight secure and simple to use with little to no learning curve, making them the ideal solution for mobile users.

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

CEOCFO: *Mr. Kim, what is the concept at DataLocker?*

Mr. Kim: Data Locker develops encryption solutions. We encrypt portable storage devices, systems and cloud storage services as well as optical media.

CEOCFO: *What is different, better, cheaper, more efficient about your solutions? Is there an overall thread that is a bit different?*

Mr. Kim: Our secret sauce is that our core design principle is "Simply Secure". We want to develop systems that are easy to use, easy to implement and easy to maintain. That is because we really believe that the weak point in most security system is actually the implementation and end user error. Therefore, our design principle solely revolves around keeping it simple and keeping it secure.



Jay W. Kim - President

CEOCFO: *How do you keep it simple? How do you really ensure a user friendly system?*

Mr. Kim: For example, for our encrypted external storage devices, our DL3 hard drives and our DL Enterprise drives, one of the key features is the fact that it has no software and no drivers. Therefore, in order to use the device you just had to have a computer that support USB mass storage. There is an imbedded touch screen display on the device itself. Through that panel you authenticate, which means you enter in your password, you manage the device, set critical security parameters and do everything at the device level. It really makes it idiot proof in the sense that you cannot use that device without properly using the cryptography. There are many other products which you can use without turning on the crypto or having some security features disabled. We really make it very simple through simple touch screen interface to really use the full capability security features of the device.

CEOCFO: *Who is using your devices today?*

Mr. Kim: We sell to government and military around the world. We have users in twenty-two different countries. We have customers like institutions like the Federal Reserve Bank, Lloyds Bank and healthcare institutions. We have a variety of customers of all shapes and sizes however roots are really within the defense industry: the military and US government.

CEOCFO: *How were you able to break into that arena?*

Mr. Kim: We received some government certifications and validations that at the time, no one else had. Therefore, we were the first manufacturer to have a FIPS validated external hard drive where the whole device is validated, not just the crypto module. Basically, when we get published out on these government approved product lists, at the time we were the only one on it. That is really what made it easy for us to jump into those markets.

CEOCFO: *How did you know when you founded the company that this is an area that you should be in? What was your incentive, your impetus, your idea?*

Mr. Kim: When we started this business, we were actually targeting a completely different market than the high security market. We were actually going after the privacy, I do not want to say gadget market, but more consumer friendly, consumer focused market. We did not realize the need for the high security market until mid 2009 when there was a series of data breaches with the US Navy and Air force and the government put a really big focus in to data security and data encryption.

CEOCFO: *Would you tell us about some of the other products that you offer?*

Mr. Kim: I think the most exciting area that we are developing now is cloud storage. We have a cloud encryption gateway product called SkyCrypt. Again, it follows our same design principal about "Simply Secure". It ties in with your cloud storage provider, whether it be Dropbox or Box or Google Drive or Bitcasa. It will link up with that and it will create a virtual drive on their system. Then you can point any application, whether it be Office or QuickBooks, whatever it may be. You just save and read from that special virtual drive location. So just by doing that you have created this rock solid layer of military grade encryption.

CEOCFO: *How do you get people to believe? How do people not see cloud as another layer of danger?*

Mr. Kim: It is right now. It really is. Given the number of breaches and if you just look at the scope of the US surveillance NSA programs, nothing on the cloud is private. You should not assume that there is any privacy on the cloud. However, that is why we created SkyCrypt. SkyCrypt encrypts the data at your desktop, so that everything going through the internet up to the cloud is being transmitted fully encrypted. When it sits on the cloud service provider, like it sits at Dropbox at rest it is fully encrypted and when you retrieve it, it comes back to you fully encrypted and then it is fully decrypted at your desktop. Therefore, even if the NSA is in the backdoor of Dropbox or Dropbox itself is hacked, the only thing that they can see of yours is fully encrypted data. Therefore, I think this mistrust for the cloud is really opening the door for products like SkyCrypt. We recently returned from the RSA Show and cloud encryption is a huge field. You are correct; no one trusts it and you really should not. However, what you can do is you can put together a program or application or a security policy that, number one, minimizes your risk or exposure to the cloud and number two, really have a good understanding of what you are putting up there and what you are not putting up there. I think that by doing that you can safely use the cloud.

"No one really wants to have to use encryption. They need it." - Jay W. Kim

CEOCFO: *Would you tell us about how you work with healthcare? Is that a growing field for you?*

Mr. Kim: Healthcare is actually one of our fastest growing markets. Last year we acquired some technology from Imation. The technology enables us to create what we call self encrypting CD's and DVD's. One of the big things that we saw within healthcare is that patient records are still delivered via optical media. When you go request medical records or a copy of an MRI or an X-ray from your doctor's office or your imaging center, they still deliver it to you on optical media. They put your MRIs on a CD or DVD and carry it up to your personal physician or you carry it to wherever you have your next appointment. We saw that that is really the standard practice. That is unencrypted media. The problem is, I guarantee that people are going to lose that. It is going to get misplaced. There is no control in terms of who is actually looking at those records. That is an area that is covered by HIPAA. Therefore, we have a solution called EncryptDisc, which basically will allow anyone at the provider to create a fully encrypted CD or DVD without installing any software or without having any special equipment. Then, the beauty of it is that anyone can read that same disc with any standard Windows computer. Neither the creator nor the recipient of that data has to have any software installed. It runs a portable encryption application that is coded on the media itself. All you need to access it is the correct user password.

CEOCFO: *When you are talking with potential customers, do they understand the difference immediately or are they so skeptical?*

Mr. Kim: No, they understand. That is because no one buys encryption out of convenience. No one really wants to have to use encryption. They need it. They need it for a variety of reasons. Number one is regulatory compliance. These days Sarbanes-Oxley, HIPAA, Homeland Security all have provisions and requirements for storing data at rest. Therefore, these are the markets that are driven by internal policy or security policy. That is probably the primary driver for people seeking encryption solutions. It is just such a prevalent issue in today's society. If you go back to WikiLeaks and look at Snowden and the NSA, all of those things could have been averted if encryption was properly used and in place. None of that would have happened if that data was properly encrypted.

CEOCFO: *What is the competitive landscape?*

Mr. Kim: We are unique in the fact that we touch upon a variety of different of end points. We offer encrypted storage, portable storage, encrypted cloud, encrypted systems and encrypted media. We have competitors in each of those areas, but not the same one for each end point. There is no one else who really competes with us across all four markets. For example, encrypted flash drives; the primary competitors are Imation or IronKey. They are an established market leader and we compete with them in that space. Encrypted cloud; there are dozens of cloud encryption gateway providers. We are a little bit unique with the way we implement and the way that you can use our service. You can actually stream video through our encryption gateway, which cannot be done with anyone else's encrypted media. We have basically got an exclusive on that market. Again, it is such a hot area and area of focus. Literally daily, we are seeing competitors in each one of those markets.

CEO CFO: *How do you reach potential customers?*

Mr. Kim: Word of mouth is probably one of our greatest regenerators. We do many industry specific events. Recently, we did the HIMSS show in Orlando for the healthcare segment. It is really important for us to get in and meet face to face with our customers. That is because once they see our technology and once they see how we implement it, it is pretty self explanatory in what we can offer. We really feel it is important to get our product in front of actual people.

CEO CFO: *Do you sell directly or do you work through channel partners as well?*

Mr. Kim: We are really committed to the channel. Our products are available through distribution. We go through most of all of the major resellers. We also sell direct, some. We have some specialty retailers that we work with as well. We have multiple GSA contract holders. We are committed to the channel and working through our partners.

CEO CFO: *How is business?*

Mr. Kim: Business is good! When we launched in 2010 and were in R&D mode for 2 years before that. The amount of awareness and the amount of interest in encryption has had huge growth in the last three, four years, it is just mind boggling. In 2010, very few people understood what encryption had to offer and why they would need encryption. Today it is on the tip of basically everyone's tongue at every trade event. Therefore, we have ridden that wave and come through that unscathed.

CEO CFO: *You are in many countries worldwide, but are there areas where you would like to have a greater presence or you think it makes sense to have a greater presence?*

Mr. Kim: I would say that one of our weakest markets, relative to the size, is the US market. We find that compared to the European market, US companies have not really embraced some of the security measures that the Europeans have. We are seeing it happen later. There is a little bit of a lag between the time the government adopts a standard and corporations do. We have found that, for example, in the EU, all of the major health systems, all of the major big financial institutions implemented requirements for data encryption probably two or three years before the American companies. Therefore, we are watching this wave come through to the US. It is really picking up here, but it is just unfortunate that it is kind of lagging behind Western Europe.

CEO CFO: *What have you learned as Data Locker has grown and developed business wise that has changed from your initial concept?*

Mr. Kim: The speed to market is probably one of the most important things. Being first to market is not always the best. When we deliver something to the market, we want to have it market ready. It has to be consistent with our core design principals of keeping things simply secure. No matter how great your technology is, if people cannot use it, it will not sell. We have seen that time and time again. That is one of the reasons why we have actually missed some opportunities with some products, because it does take more time. It takes more design commitment in order to deliver a product that is really simple to use. One of the good examples is that we have been in art development on an NFC authenticated encrypted flash drive. We have been working on that for well over a year now. It is just something to perfect the technology in terms of making it really intuitive and really simple to use. Therefore, rather than just throwing it out there we are really taking our time. We want to get it right. Again, we believe if it is easy to use people are going to use it. If not, it is not going to do well.

CEO CFO: *Why pay attention to DataLocker?*

Mr. Kim: It is evident the problems that our solutions can address. What you really have to think about is cost of implementation and how thoroughly these solutions are rolled out. Again, our design principle is keeping it simply secure. We want to make things as easy to use and as accessible to users as possible. We really believe that will strengthen any companies overall security policy.

BIO: After founding the company in late 2007, Jay led all phases of product development, funding and growth of DataLocker. DataLocker currently sells products in over 20 countries to companies and organizations such as the Federal Reserve Bank, all branches of the US military, Total Oil, and Lloyds Bank. Prior to founding DataLocker, Jay served as Managing Director of QMD International, a tier one supplier to the home appliance industry. Jay has been involved in a variety of businesses in the e-commerce, healthcare, international trade and pharmaceutical markets.



Data Locker
7500 College Blvd Suite 1200
Overland Park, KS 66210
913-310-9088
www.datalocker.com