How Smart Data Fragmentation will Change the World

Fred Callis
CEO & President

Cybervore, Inc.
www.cybervore.com

Contact:
732-829-8899
fcallis@cybervore.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: *Mr. Callis, what is Cybervore™?*
Mr. Callis: Cybervore is a cybersecurity software company. We make a product called Fragglestorm™ which provides a secure method to help businesses transition their data to cloud services. How secure? It makes data useless to any unauthorized person- only an authorized user can access their data. Cool, right?

CEOCFO: *How does Fragglestorm go beyond encryption?*
Mr. Callis: Well, encryption jumbles the actual data but keeps the data all together. Through certain brute-force technologies, today's encryption can be compromised. Soon, through the commercialization of quantum computing, encryption will become handicapped and broken.

To protect and manage data in today's multicloud services world, the Fragglestorm process takes the actual data, uses the encryption but then fragments the data into multiple puzzle-like pieces. We then wrap technology around those pieces, thereby making the 'data smart', which by the way, we call Smart Fragments™. As such, these smart fragments become impossible to break or reassemble unless you are the authorized user.

For example, if a document was stolen or compromised in any way, even if the encryption is broken, the hackers only have a very small piece of the puzzle. It gets better. Let's take lots of data in general and all of these are turned into smart fragments. If we dump them all together, you can start to see how hard it is to hack through or try to break them. Finally, let's make it even more difficult. Let's place those pieces in different locations across storage devices or cloud services. As a result, Fragglestorm allows the data to become ultra-secure and hardened against being broken or useful by any bad actors.

CEOCFO: *Is this a novel approach? Has it been tried before? Is it in use now in other ways?*
Mr. Callis: Yes. Think of how data is stored on a disc drive on any computer. Data is separated into pieces on a disc drive which allows the data to be stored more efficiently. However, when you put data on a network or cloud service, you are outside the data center which is why businesses are so concerned about security and resiliency. Regarding how it is in use in other ways, up until recently, encrypting the data was good enough. But times are changing and we believe

encryption plus Fragglestorm can fill the void specifically against encryption-breaking systems such as quantum computing.

Our approach enables the fragments themselves to reassemble into a file when authenticated credentials are presented. In today's marketplace other companies may use fragmentation, but no one has developed software that simultaneously assures availability, accessibility, security and ransomware recovery into one product.

CEOCFO: *How do you create a system that will do this? How do you separate the data and how do you put it back together?*
Mr. Callis: It is based upon mathematical algorithms and processes. There is a lot of detail that goes into how fragments are made and how they are made smart. They are connected almost a little bit like the blockchain concept, but it is not public blockchain. It is more of a private blockchain built for performance. As such, a smart fragment would know another smart fragment; how they all go together. You cannot even come up with fake fragments, because they are intelligent to each other. Awesome, right?

CEOCFO: *Who is using this?*
Mr. Callis: Right now we are a software startup. We have early adopter customers that wish to remain anonymous and we have a product release scheduled for the end of this year.

CEOCFO: *Who would be the most likely types of companies, industries or size of organizations that you would be targeting? Who needs this more than others?*
Mr. Callis: Our initial target market is small to medium-size businesses. They are the biggest targets of cybercriminals and we can help them the most. As far as industry verticals: healthcare, financial services, and legal/accounting.

> **"Fragglestorm is as disruptive a technology to cybersecurity as the disk drive was to the computer."- Fred Callis**

CEOCFO: *Would you be working through MSPs or would you be looking at reaching the end customer directly?*
Mr. Callis: We work through both MSPs and carriers to offer Fragglestorm. They are market-positioned between their users and cloud services which makes them ideal to work with. Fragglestorm offers MSPs and carriers new ways to further protect their customers as they transition their data to multiple cloud providers. To them, this is a competitive value.

CEOCFO: *When you are speaking to the right person, do they recognize the concept and the effectiveness?*
Mr. Callis: Yes. The example I use is: take your name and social security number as one saved document. By using Fragglestorm, the document is encrypted and then fragmented. Those pieces are wrapped in our secret sauce, copied or replicated as well as versioned into multiple copies. These pieces are then intelligently stored across different locations which could include on-premise devices, PCs/servers, or multiple cloud services. The value here is even if the data is stolen, the hackers only have a piece - if they can break it. That is how Fragglestorm makes data ultra-secure and manageable anywhere.

CEOCFO: *Would this be in conjunction with other security measures? How does this come together?*
Mr. Callis: We complement other security solutions - we do not replace them. In other words, sometimes the hackers get in or a virus infects computers and servers. They will always need other security products to help them. We are the last line of defense. What we do is make the data useless to any unauthorized user no matter where the data is located; only an authorized user can access and reassemble their data.

CEOCFO: *Are you seeking funding, partnership or investment as you move forward?*
Mr. Callis: Yes. We need money to grow. We have a great management team which is experienced in building new businesses. But in this cybersecurity marketplace, rapid growth requires capital and strategic alliances. It takes a village. We are in a business where hopefully, a.k.a. through hard work, we can align with the right lead investment firm.

CEOCFO: *When did you recognize that this was the way to go as a product? When did you recognize this was something needed and that you could do it?*
Mr. Callis: About two years ago, we were awarded a patent for Smart Data Fragmentation™ after years of researching and looking deeper into the security and management of data. We found so many businesses were getting hacked or ransomed regardless of all the security products they had installed. We also noticed that corporate hacks and breach reports were showing up on national and global news channels, not just on tech news.

With the rise of quantum-computing which greatly handicaps encryption and the ongoing exposure to financial penalties, legal, and compliance problems, we concluded there is a huge growing market place for smart data fragmentation.

CEOCFO: *There are so many ideas to look at regarding cyber security. Why Cybervore now?*
Mr. Callis: Data is a business's most important asset and it is also a huge liability. Today's basic business operations and intelligence require data to be safe and resilient. If they cannot get to their data to make decisions or operate, they are out of business. This is especially true for small to medium-sized businesses which are the fastest-growing piece of the U.S. economy.

Fragglestorm can help businesses simplify their access to multiple cloud services while keeping their data safe because there is protection no matter where the data is located.

We are evolving into a cloud services mobile world where data needs to be as intelligent as the systems and networks that process it. Cybervore hopes to be a big part of this movement with Fragglestorm. Thank you for the opportunity to be featured in the CEO/CFO magazine.