Dr. Roger Billings Speaks About The Increasing Importance of Serious Cyber Security

We had the privilege of getting to know Dr. Roger Billings, Founder and CEO of CybrSecurity Corporation. While he is perhaps best known for inventing the first hydrogen-powered car, for the past 30 years he has focused on high tech companies. Some of his ventures include pioneering Gigabit Ethernet over copper (full-duplex mode), GoldKey Security, and the Acellus Learning System. Currently, with CybrSecurity Corporation, he spends his days tackling better cyber security. Learn more about Dr. Billings and his work at CyberSecurity Corporation here:

Q: Tell me a bit more about your background and the work that led you to this place.

RB: In the mid-1970's, with the advent of the microprocessor, I saw the potential and created the Billings Microsystem, a single user computer with the CPU, monitor, keyboard and disk drives all in one cabinet. The system was complete with software, which included an award-winning word processor, spreadsheet and even

e-mail.

I am also responsible for the technology known as client/server computing, for which I received a foundational patent. This networking system is in worldwide use today, enabling millions of users to share data locally, in the enterprise, and via the Internet. The Internet of today, with its plethora of functions and services, is made possible by this foundational networking infrastructure.

In answer to today's vital need for strong data security, I have founded the company CybrSecurity Corporation, which offers b2 Cryptography, the enabling technology behind the strong GoldKey Security. GoldKey has become one of the most robust yet securely versatile cybersecurity systems in the industry and has been deployed by the military, by business, and by educational institutions across the nation and around the world.

Q: Cyber security is a hot topic now, more than ever. Why is your solution unique and how does it compare to competitors' products?

RB: The thing that makes our solution so unique is b^2 cryptography. b^2 cryptography is serious security. PKI or Public Key Infrastructure is the cryptographic technology which the military and large enterprises have relied on for over 30 years, and it can be compromised.

More recently, Certificate Authorities were developed to fill the weakness of PKI not providing authentication. However, the chain of trust these rely on has been broken, especially when you look at the revocation and recovery processes. They are also very complex to manage often leading to breaches due to configuration issues.

CybrSec b^2 Cryptography is an industry disruptive technology that has solved the age old problem of securely exchanging encryption keys, even over a hostile public network. b^2 cryptography utilizes portable security tokens that are connected in a hierarchical structure. Authority inside the hierarchy is delegated in chain of command style deployment from the top down. With the hierarchy established users can share encrypted data within the hierarchy.

A crucial element in b^2 Cryptography is the ability to really authenticate the true identity of a user. As a security token is assigned to a user, a verifiable identity is associated between the token and user. When authentication is required, the user must provide their assigned token and verification of their identity. This can be as simple as entering a PIN, or for more secure applications the user may be required to provide a biometric or multiple factors of authentication.

This is why b^2 cryptography is serious security.

Q: Why is your solution relevant with Department of Defense and/or smart cities?

RB: The CybrSec Solution provides important benefits to the Department of Defense. There is no question that cybersecurity has become the new battlefield over which our military must gain a tactical advantage. Cyber adversaries and state sponsored groups have been able to break our most widely deployed cryptography and gain access to military personnel records, battlefield intelligence, and our most secure networks.

CybrSecurity b2 cryptography is the cryptographic technology behind the **2018 Defense TechConnect** Innovation Challenge award-winning "Warfighter Authentication and Secure Communication (WASC) System". The major breakthrough in b2 cryptography is the ability to securely exchange encryption keys even over public networks. This disruptive technology is revolutionary in its ability to allow military leaders and warfighters to make data-driven decisions at mission speed over any network with stronger than air-gapped security.

The CyberSec solution utilizes GoldKey security tokens, fs·ix secure servers, and WideBand nano-latency networking products. This provides the DOD with a completely integrated solution combining extreme security with extreme performance that is easy to use, can be deployed on top of existing security systems, and offers a simple deployment path with commercially available devices.

Q: If you could wave a magic wand and endow the general population with some piece of information about security, what do you think would be the most useful and most impactful thing for them to know?

RB: I think people would be alarmed if they understood how vulnerable our data and communications are to cyber attacks. With every major breach in the news, more and more are beginning to realize the consequences of weak security and demand better. Over the next ten years, I think we are going to see how essential cybersecurity has become.

Q: Tell me about a project or partnership you're especially proud of and why.

RB: We have been working with the United States Navy for about five years now. During this time, they have been using CybrSec b^2 cryptography to provide multi-factor authentication for some of their most secure systems. More recently they have started using CybrSec Secure Communications for secure email, encrypted phone and text messaging. They are also utilizing the CybrSec Encrypted Cloud Storage. This allows them to collaborate with vendors, partners and organizations such as academia outside of the Navy security infrastructure and still maintain a high level of security. This relationship really shows the strength and usability of the technology.

Q: What are the three most important steps a city or agency should consider as a starting point for becoming adequately secure?

RB: Implementing multi-factor authentication should be a major priority for these organizations. According to Verizon, 81% of the data breaches that occurred last year involved a weak or stolen password. Those breaches could have been prevented with stronger authentication.

Government agencies also need to be cautious about putting data into the cloud. Sensitive data stored in the cloud should be protected with AES 256-bit encryption in addition to multi-factor authentication.

Careful consideration should also be given to the security of communication within these organizations. A large amount of sensitive information is communicated via email, in text messages, or even through video chat. Securing these types of communication is another critical step that these organizations need to take.

Q: With the Defense TechConnect Conference coming up in Tampa, what do you hope to accomplish on site?

RB: In many ways it has already been a successful show for us. It was wonderful to hear that CybrSec received the 2018 Defense Innovation Award from Defense TechConnect for the CybrSec Warfighter Authentication and Secure Communication System (WASC). Receiving that recognition is a good start to accomplishing our goals.

I have enjoyed interacting with the other innovators on the DOD Innovation Keynote Program. I am impressed with the caliber of individuals and organizations represented and look forward to being part of the panel discussion on the opening day of the conference. I believe our b2 cryptography is poised to make a big impact in providing more robust security for our military networks and communications.

Q: Considering how far we've come, technologically, and how much is still ahead, what do you think will be the next frontier or next breakthrough in cyber security? Why?

RB: CybrSec's b^2 cryptography is a game changer in its ability to securely exchange encryption keys over public networks. This disruptive technology has the power to revolutionize the tactical edge we provide to today's warfighter.