Robert R. Ackerman, Jr., Managing Director and Founder, Allegis Cyber, Talks About Cybersecurity Threats, Solutions

And Best Practices "In The Boardroom" On SecuritySolutionsWatch.com

Robert R. Ackerman, Jr., Managing Director and Founder, Allegis Cyber

NEW YORK, NEW YORK, UNITED STATES, February 14, 2019 /EINPresswire.com/ -- SecuritySolutionsWatch.com: Thank you for joining us today, Bob. It's an honor to speak with the "father of the 1st iPhone" (http://www.internethistorypodcast.com/2015/06/the-forgotten-story-of-the-iphone-released-in-1998/) . You've seen it all and heard it all ! Before discussing AllegisCyber in greater detail, please give us a brief overview of your background.

Bob Ackerman: I'm the founder of AllegisCyber, a seed and early-stage venture capital firm investing in cybersecurity companies. I'm also a co-founder of DataTribe, a start-up studio building successful cybersecurity companies in Maryland.

I founded Allegis Capital in 1996 after a successful career as a serial entrepreneur. In 2013, building on the firm's historic success in cyber security investing and recognition of its effective focus on cyber, I subsequently changed its name to AllegisCyber. The firm was both the industry's first venture firm to focus exclusively on cyber security innovation and we raised the industry's first dedicated cyber fund in 2015.

My founding mission for AllegisCyber was to build a seed and early-stage venture firm that would combine operational expertise with entrepreneurial spirit and a focus on forging partnerships with portfolio companies to build successful, sustainable cyber technology companies.

> We are honored to have Bob Ackerman, Managing Director and Founder, Allegis Cyber, join us "In The Boardroom" to talk about cybersecurity threats, solutions and best practices."
>
> *Martin Eli, Publisher*

I then co-founded DataTribe in 2015. DataTribe, based in Maryland, co-founds and grows cyber and data science technology startups, in partnership with subject matter expert engineers coming out of the U.S. intelligence community and U.S. national labs. I'm happy to state that i was recognized as Fortune 100 cybersecurity executive and also as one of "Cybersecurity's Money Men."

Prior to founding AllegisCyber, I was President and CEO of UniSoft Systems, a leading UNIX systems house. I was also the Founder and Chairman of InfoGear Technology Corporation, a pioneer in the original integration of web

and telephony technology and the creator of the original IPhone, as you mentioned.

Outside of AllegisCyber and DataTribe, I taught New Venture Finance in the MBA program at the University of California for years. I currently co-manage my family's Napa Valley winery—Ackerman Family Vineyards—and I'm an avid fly fisherman.

SecuritySolutionsWatch.com: One will read at Allegis Cyber that, "...we are "company builders" who think in term of "unfair competitive advantage" for entrepreneur partners (https://allegiscyber.com/our-advantage/) .
Care to elaborate?

Bob Ackerman: We are not just finance guys giving money to entrepreneurs – we build companies. We combine decades of successful entrepreneurial, operating and venture investment experience. Our team of Venture Partners are proven industry veterans, each with decades of entrepreneurial success, building some of the market's most successful companies. Our operating playbook leverages this experience together with our market, technology and domain expertise, customer, entrepreneur and investor networks to help our entrepreneurial partners accelerate their growth, reduce start-up risk, lower overall capital requirements and improve the probability of market success.

Building a start-up company has been likened to running through a mine field, naked, in the middle of the night. The odds against success are long. Our playbook delivers a "map through the mine field" to our entrepreneurial partners, translating to an "unfair competitive advantage" in challenging, dynamic, complex and rapidly evolving market.

SecuritySolutionsWatch.com: The Allegis Cyber Portfolio (https://allegiscyber.com/portfolio-new/) is indeed quite impressive with some very well known brands and some lesser known brands. We've got plenty of time and plenty of ink...want to give us a brief thumbnail of each company?

Bob Ackerman:
Area 1 (https://www.area1security.com/) provides performance-based cybersecurity that blocks phishing attacks that other solutions miss.

Callsign (https://www.callsign.com/) provides real time AI-driven Identity and authentication solutions that confirms if users really are who they say they are.

CyberGRX (https://www.cybergrx.com/) is dedicated to helping organizations streamline their third-party cyber risk programs.

Dragos (https://dragos.com/) provides an industrial cyber security platform that delivers unprecedented visibility and prescriptive procedures to respond to adversaries in the industrial threat landscape.

Safeguard Cyber (https://www.safeguardcyber.com/) provides end-to-end digital risk protection. Their platform is a single solution to detect, prevent, and defend against threats in all of a customer's digital channels.

Shape Security (https://www.shapesecurity.com/) uses artificial intelligence to defend against automated BOTnet attacks.

Source Defense (https://www.sourcedefense.com/) provides a unique solution to prevent website supply chain attacks leveraging automation and machine-learning.

Synack (https://www.synack.com/) is a human-powered security solution offering scalable continuous testing for enterprise applications and networks.

DataTribe companies:
Attila (https://attilasec.com/) mobilizes security at the edge where cyber threats matter. Their GoSilent technology was designed to protect government and enterprises from advanced cyber attacks, zero-day threats, and personal identity theft.

CyberWire (https://thecyberwire.com/) is an independent voice delivering concise, accessible, and relevant cyber security news to people all across the globe.

Dragos (https://dragos.com/) provides an industrial cyber security platform that delivers unprecedented visibility and prescriptive procedures to respond to adversaries in the industrial threat landscape.

ENVEIL (https://www.enveil.com/) uses homomorphic cryptography to secure data-in-use, including data interactions, search and analytics.

Inertial Sense (https://inertialsense.com/) provides high precision micro-navigation solutions for a world that is beginning to move on its own.

Prevailion (https://prevailion.com/) is the first business compromise intelligence platform that provides actionable notification and definitive characterization of successful compromise.

ReFirm Labs (https://www.refirmlabs.com/) is a group of IoT security experts who have developed a new method for vetting and validating firmware.

SecuritySolutionsWatch.com We're all familiar with the headlines about
Cryptolocker - NotPetya - WannaCry:
https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html

Equifax: https://www.ftc.gov/equifax-data-breach

Ticketmaster: https://www.zdnet.com/article/ticketmaster-breach-was-part-of-a-larger-credit-card-skimming-effort-analysis-shows/

Uber: http://fortune.com/2018/04/12/uber-data-breach-security/

My Heritage: https://www.reuters.com/article/us-myheritage-privacy/security-breach-at-myheritage-website-leaks-details-of-over-92-million-users-idUSKCN1J1308

Orbitz;https://www.usatoday.com/story/tech/2018/03/20/800-000-orbitz-cards-compromised-breached/442277002/

and the ransomware attack on the city of Atlanta: https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html

What is your perspective, please, regarding best cyber practices that should be followed by the public and private sector in this environment?

Bob Ackerman: Timely advice about creating a worthwhile corporate cybersecurity strategy

sagely starts by realizing that establishing firewalls and relying on the IT department to monitor attacks isn't sufficient. Reactive strategies break down over time, making proactive strategies crucial.

Further, defensive strategies work only within centralized, controlled and managed-device networks – all now tottering on the edge of extinction amid the proliferation of cloud computing, the Internet of Things (IoT) and mobile technology.

Experience continually reinforces the reality that the human element is the weakest link in cybersecurity. This means the most important proactive strategy of all is to train everybody in a corporation – and I mean everybody – in good cybersecurity practices, along with their contractors and vendors. All employees should not only understand what is expected of them regarding company security policy and good online behavior, but also be trained to spot nefarious or suspicious activity and to conduct periodic tests to ensure best practices are followed.

It is employees, after all, who are the first – as well as the last – line of cyber defense.

Corporations need to balance technological deterrents with agile, human-centric defenses. This is instrumental because cyber technology continually evolves, which means purely technological solutions cannot keep pace. In addition, it is much tougher to play defense than offense, and attackers, unlike defenders, have patience on their side. And, too, many attackers are typically as knowledgeable as corporate cybersecurity pros and only to have to be right once to be successful, while cyber defenders have to be right all the time.

Regardless, it is best to assume that defenses will be compromised at some point – no organization is cyberattack-proof – and to train employees what to do when that happens. The sustainability of the business ultimately hinges on what every employee, internally and externally, does.

Training alone, of course, isn't sufficient. Once it's in place, corporations also need to create a highly tailored cybersecurity strategy.

Companies must reevaluate how their systems and networks are used and who uses them, and then implement a feedback loop. It would be wise to start with technical assessment of current areas of weakness and then follow up with a review of non-technical matters. The technical assessment helps identify vulnerabilities within the network. Policy and employee assessments help identify non-technical areas that need to be assessed. It is essential that this process be open ended and repeated regularly. Networks are dynamic. Assessments also must be.

Specific security programs then need to be implemented, plus steps to assure follow-through, such as the application of software updates and patches to help minimize vulnerabilities. Policies should also identify roles and responsibilities, including acceptable use conditions for employees, and a point person needs to be chosen to make sure these are implemented and maintained.

Employees must be taught to recognize deceptive cyber ploys and other common threats to help enable them to act as the first line of defense against cyber attacks. In addition, they should be instructed about safe password management and secure browsing practices.

Along the way, both technical and non-technical players should participate in shaping a security strategy. The technical folks ensure that the plan satisfies the needs of IT and business operations. Non-technical folks, meanwhile, are usually better at nudging employees to take corporate cybersecurity policy seriously and at monitoring employee cyber policy.

Corporations also must establish protective monitoring to prevent and deter "insider" threats,

whether intentional or accidental. This provides an over-arching view of cyber activity throughout the corporation and supports a positive culture to deter bad behavior. And, of course, it helps companies combat the threat posed by insiders.

Most important of all, corporations and other organizations must build a solid and highly tailored cybersecurity foundation – i.e., a sound analysis of security capabilities from a bottom-up, device-centric perspective. The application of traditional firewalls, intrusion prevention systems and multi-factor authentication (moving beyond two factors), for example, typically needs to be tweaked or changed substantially, depending on the devices and nodes used in a corporation.

Also part of a good foundation is an appreciation of context, which is how the network interacts with particular devices, as well as the realization that corporations must play offense, as well as defense.

Regarding context, company security staffers must determine which network nodes they can control and which they can merely observe in an advantageous manner. IoT devices, for example, offer the least control. Companies with lots of these might want to consider the so-called "ring-fence" approach. This entails drawing a perimeter around devices that require access to similar resources in an effort to better monitor overall cyber behavior and react more quickly to problems.

Offense is often as important as defense because it helps instill a mindset of continuous cybersecurity improvement. Corporations should regularly challenge the quality of their cybersecurity defenses via proactive testing, commonly known as "red team, blue team exercises." Penetration tests and threat modeling, for instance, enables a red team to challenge lower-profile attack avenues to better understand their vulnerabilities. Defense-oriented blue teams, meanwhile, can help fix the security weaknesses unearthed.

When the development and implementation of a cybersecurity strategy is completed, companies should take the trouble to gauge whether it is sufficient.

Here is an informal checklist:
Is cybersecurity policy driven from the top of the organization? A strong cyber strategy is a core corporate message, and it is driven by senior management. Remember, cyber security is about risk throughout the enterprise. IT is simply the vector.

Does cybersecurity come up at or near the start of every meaningful IT discussion? It's much easier to implement cybersecurity early in the lifecycle, rather than as an add-on.

Is cybersecurity communicated in basic English? Every employee should understand what they need to know about cybersecurity. "Geek speak" is a no-no.

Has your company established a predictive security edge? Do you have the wherewithal to anticipate your adversary's next move?

Does your data security system work in harmony? In other words, do your people, processes and technology work well together?

Are there ample "change agents" spread throughout the corporation? Advocates help spread the cybersecurity vision across the enterprise.

Does your corporation embrace cybersecurity? Cybersecurity is part of your cultural DNA. As such, it's factored into all business decisions. Your organization naturally embraces good cybersecurity policies – without a second thought.
The current state of cyber security is heavily focused on defending IT infrastructure vulnerable to

cyber compromise and mitigation and remediation in the event of a cyber attack. While this current focus is necessary and essential, longer term, we need to shift our focus to securing and ensuring the integrity of data, which in itself is most often the target of a cyber attack. This "data-centric" approach to cyber will lead the next wave of integrated cyber security through data science innovation.

SecuritySolutionsWatch.com: May we ask you, Bob...what does your crystal ball reveal regarding cybersecurity headlines in the coming year?

Bob Ackerman: Here is a mini dive into the top pending threats.....

For the balance of this interview with Robert Ackerman please click here:
http://www.securitysolutionswatch.com/Interviews/in_Boardroom_Ackerman_AllegisCyber.html

For more information about Allegis Cyber: https://allegiscyber.com/

****

M A R K - Y O U R - C A L E N D A R !!!
SecuritySolutionsWatch.com Is Proud To Be A Sponsor Of ...

CYBER INVESTING SUMMIT
Thursday, May 16, 2019
Convene – Financial District
32 Old Slip, New York, NY 10005

Videos of previous CYBER INVESTING SUMMIT here:
https://www.youtube.com/channel/UCCi2WTHuC8h2nIba2jyA2Jg
https://cyberinvestingsummit.com/

****
About SecuritySolutionsWatch.com

www.SecuritySolutionsWatch.com features thought leadership interviews about IT, IoT and security solutions. Our flagship "In The Boardroom" program, now in its 15th year, has delivered outstanding content about solutions from leading global brands such as: 3M, AMAG Technology - A G4S Company, ASSA ABLOY, Cisco Security, Cyberinc, Dell EMC, HP Cybersecurity, Fujitsu, Gemalto, HID Global, IBM, ImageWare, Intel, SAP, Siemens, Stanley Security, SONY, Unisys, and Yahoo, just to name a few.

What's YOUR authentication, cybersecurity, physical security, mobility, or "smart" solution?

What's YOUR Blockchain or FinTech solution?

We invite you to please join us "In The Boardroom" at www.SecuritySolutionsWatch.com.

For a quick tour to see exactly how your brand will be featured, please contact Ali Eng on our publishing team via
email: ALE@SecuritySolutionsWatch.com, or phone: 1+914.690.9351, or, LinkedIn:
https://www.linkedin.com/in/ali-eng-a8a41015b/

For more details, please click here: www.SecuritySolutionsWatch.com/Main/Jan2018.pdf

And for our Media Kit, please click here: www.SecuritySolutionsWatch.com/MediaKit.html

****
It's FREE...our monthly newsletter with thought leadership content from leading security experts.
Please click here: www.SecuritySolutionsWatch.com/newsletters/newsletter_2019_01.html
And please visit us on Twitter here: www.twitter.com/SecStockWatch

****

All content which appears on SecuritySolutionsWatch.com and in this Press Release is subject to our disclaimer:
www.SecuritySolutionsWatch.com/Main/Terms_of_Use.html

****

Martin Eli, Publisher
SecuritySolutionsWatch.com
+1 914-690-9351
email us here
