

- [Home](#)
- [About](#)
- [Advertise](#)
- [Glossary](#)



Search in this site...

GO

- [News](#)
- [Contract Awards](#)
- [Executive Moves](#)
- [M&A Activity](#)
- [Financial Report](#)

Mark Gerencser Named CyberSpa Chairman, Retires as Booz Allen EVP

Posted by [Tim Watson](#) on Jul 8th, 2013 // [No Comment](#)

Like

Tweet

Share



[Mark Gerencser](#) has retired from his position as an executive vice president at [Booz Allen Hamilton](#) (NYSE: BAH) after a 31-year career with the Tysons Corner, Va.-based contractor and joined PC services company [CyberSpa](#) as chairman of the board of directors.

Baltimore, Md.-based CyberSpa's PC services system fully automates delivery of data transfer, virus removal and other performance and security services, the company says on its website.

Gerencser helped found CyberSpa in 2010 and Allen Shay, CyberSpa president and co-founder, said he has worked with Gerencser over the last 15 years.

Allen told GovCon Wire that Gerencser will work to identify a few more executives to round out the board.

Allen added that the company looked in part to Gerencser's expertise in cybersecurity and other specialties in its efforts to enhance the firm's market position and capabilities.

The company said its system is designed to adapt future software and services to its core platform.

Gerencser served six terms on Booz Allen's board of directors over his career in addition to serving on the executive management committee and leading its partnership committee as chairman.

In his most recent position at Booz Allen, Gerencser led the global commercial and international business group. He elevated to that position after serving as managing director of the global government business.

For more on Gerencser's background, [click here to read](#) GovCon Wire's previous executive coverage.

email

Tags: [board of directors](#), [Booz Allen](#), [commercial](#), [cyberspa](#), [Executive moves](#), [government](#), [Mark Gerencser](#)

[« Previous](#)

[Gerry Fasano Named Lockheed IS&GS Business Development, Strategy Head](#)

Leave a Reply

Monday, July 8th

- [Executive Mosaic](#)
- [GovCon Wire](#)
- [ExecutiveBiz](#)
- [TNNI](#)
- [ExecutiveGov](#)
- [GovCon Exec Magazine](#)
- [POC](#)



search...

- [News](#)
- [Profile](#)
- [Tech Trends](#)
- [Exec Spotlight](#)
- [Lifestyle](#)
- [Philanthropy](#)
- [About Us](#)

You are here: [Home](#) » [Profile](#) » Profile: Mark Gerencser, Booz Allen EVP and Managing Partner for Global Commercial Business

[Profile: Mark Gerencser, Booz Allen EVP and Managing Partner for Global Commercial Business](#)

March 4, 2013 8:01 am [0 comments](#) Views:



Mark Gerencser, Booz Allen

[Mark Gerencser](#) is an executive vice president at [Booz Allen Hamilton](#), where he [manages the firm's commercial business](#) and serves as chairman of the partnership committee.

The commercial team helps financial services, health, energy and utilities clients address issues with cybersecurity, business and information technology transformation and risk mitigation.

The 30-year company veteran also advises government, private, and non-profit sectors on solving solve complex problems in infrastructure development, improvement and renewal.

He spoke to [GovCon Exec magazine](#), Executive Mosaic's print publication, on the need to re-imagine infrastructure in the [Fall 2011 issue](#).

Before moving over to the commercial business, he served as managing director of the global government business, leading the public sector business within the U.S. and abroad.

He served six terms on the board of directors and was a member of the firm's leadership team responsible for setting Booz Allen's strategic agenda, market strategy, resource allocation and major investments.

Gerencser has led Booz Allen's national security business and created its homeland security practice.

He created the commercial enterprise resilience practice serving clients in consumer, financial services, energy and healthcare industries and also created Booz Allen's Infrastructure Center of Excellence.

Gerencser has had many external leadership roles, including an industry expert panel addressing the [National Security Agency's](#) infrastructure resilience and facilitating CEO roundtables addressing interdependencies between business, trade and security.

He hosted a cyber-summit for Fortune 1000 and agency chief information officer to create a shared agenda on information privacy and assurance.

He has chaired several technology studies for the Electronics Industries Association to forecast the impact of technological change; led war games and multi-stakeholder simulations to address port security, bioterrorism, and cybersecurity challenges; and represented industry to several Office of the Secretary of Defense net assessment initiatives to help assess U.S. defense readiness.

He currently serves on a bipartisan policy center commission addressing energy security policy for the United States.

Gerencser was nominated by the White House and confirmed by the Senate Armed Services Committee as a member of the National Security Education Board, chaired by the Secretary of Defense.

He is a member of Business Executives for National Security, serves on its board of directors and was chairman of its policy committee.

He is chairman of the board of visitors for the University of Maryland, University College where he received the President's Medal in 2009 for his leadership and vision in advancing higher education.

In an essay for UMUC's Achiever magazine, he outlines the opportunities and implications for businesses as they enter the real of big data ([click over to ExecutiveBiz](#) for the full article).

Gerencser is a board member of Security Technology Institute incubating the growth of new cyber technology companies in the State of Maryland.

In 2007, Consulting Magazine named him one of the top 25 most influential consultants in the world.

ExecutiveBiz named him one of the Top 10 Game Changers in Washington D.C. for 2009 and one of the Top 20 People to Watch for 2011. Virginia Business Magazine listed him as one of the Top 25 Executives to Watch in 2011.

He has also authored numerous articles on technology and policy (Artificial Intelligence, Robotics and Robotic Vehicles, Toward a Digital Democracy, Re-Imagining America's Infrastructure) and its impact on business or national security.

According to Vital Speeches of the Day, Gerencser's keynote speech at the 2009 Cybersecurity Symposium was one of "The best thoughts of the best minds on current national questions."

He has appeared on numerous television news programs on CNN and other networks and has been featured in print media as well, including the Washington Post, Wall Street Journal and Los Angeles Times.

Gerencser holds a bachelor's degree in electrical engineering from Rutgers University's College of Engineering and a master's in technology management from the University of Maryland, University College.

Tags: [Booz Allen commercial](#) [Cybersecurity](#) [energy](#) [health](#) [infrastructure](#) [Mark Gerencser profile](#)

- [Tweet](#) { 0
- [Like](#) { 0
- 0



Author: [Ross Wilkers](#)

No Comments

Leave a Reply

Name (required)

E-Mail (will not be published) (required)

Website

- [Home](#)
- [About](#)
- [Advertise](#)
- [Glossary](#)

Search in this site...

GO

- [News](#)
- [Contract Awards](#)
- [Executive Moves](#)
- [M&A Activity](#)
- [Financial Report](#)

Booz Allen Elevates Mark Gerencser to Managing Partner for Global Commercial Business

Posted by [Tim Watson](#) on Feb 3rd, 2012 // [2 Comments](#)

Like

Tweet

Share



Booz Allen Hamilton (NYSE: [BAH](#)) announced today it has elevated 30-year company veteran [Mark Gerencser](#) to managing partner for its global commercial business.

Gerencser most recently served as Booz Allen's executive vice president, leading the firm's efforts to solve complex energy, environment, transportation and infrastructure problems.

Booz Allen said Gerencser's new post will be essential to driving growth in an era of declining defense and federal budgets.

"Firms with diverse market presence and the right capabilities are better positioned for future success in the changing and turbulent world that we all face," Gerencser said Friday.

Gerencser has served six terms on Booz Allen's [board of directors](#) and serves as chairman of the firm's partnership committee.

Prior to assuming the EVP post, Gerencser created Booz Allen's [homeland security practice](#) and lead its domestic and international public sector business.

He also created Booz Allen's Infrastructure Center of Excellence.

In the early 2000s, Gerencser helped grow several of the technology and management consultant's commercial businesses in the energy, consumer, financial services and healthcare industries.

One of Gerencser's driving missions as EVP has been to maximize the results of collaboration between government, private sector and non-profit leaders.

In his best-selling book "[Megacommunities](#)", Gerencser advocates that public, private and civil sector leaders must unite to solve the world's most pressing problems.

In its earnings call today, Booz Allen released financial results for the third quarter of its 2012 fiscal year, reporting a 48 percent increase in adjusted earnings per share over the prior year period.

email

[« Previous](#)

Cyber Hunting: Proactively Track Anomalies to Inform Risk Decisions

by Richard Stotts and Scot Lippenholz, Booz Allen Hamilton

The number and diversity of cyber attack scenarios and the motivations that inspire the actors who launch them continue to escalate and challenge enterprise cybersecurity practitioners. There is no shortage of targeted victims either. Government organizations, defense contractors, critical infrastructure owners and commercial enterprises are all vulnerable to attack.

The range of intrusion methodologies includes socially engineered phishing emails used to gain access to enterprise networks, Distributed Denial of Service (DDoS) nuisance attacks to disrupt services or more serious smokescreen hoaxes to exfiltrate confidential information, and increasingly sophisticated and targeted Advanced Persistent Threats (APTs) aimed at stealing intellectual property. Adversaries include hackers, organized crime syndicates, nation-states and terrorists. Motivations for cyber warfare are rooted in political, economic military and criminal agendas.

The cyber threat landscape, now a complex tapestry encompassing this broad range of elements, has both public- and private-sector organizations in every industry sector on the hunt for tactical and strategic solutions that ensure protection of their critical assets.

ATTACK EVOLUTION SNAPSHOT: FROM WORMS TO STUXNET

Looking back, early cyber exploits, such as relatively simplistic worm attacks, were launched by amateur digital mischief makers to demonstrate technological acumen. Then it was discovered that malicious software could be profitable, and along came the first versions of DDoS attacks, followed by the “electronic Pearl Harbor” incident in 2007 in which approximately 12 terabytes of data (equivalent to U.S. Library of Congress) were stolen from federal government organizations, as described in a June 2010 *60 Minutes* segment entitled “[Cyber War: Sabotaging the System](#).” Next, in 2010, the military-grade Stuxnet cyber weapon demonstrated the ability to plant malware on networks and establish a foundation for broader, well-orchestrated future attacks to destroy critical infrastructure.

HIDDEN ANOMALIES PRESENT GREATEST DANGER

Today’s organizations are well aware of this sobering evolution and the current dynamic threat environment. They have their hands full defending against the attack du jour, but adopting a viewpoint that assumes nothing else malicious is going on beyond the current infiltration is a dangerous proposition. While all efforts and energy are dedicated to responding to the latest attack, attention is diverted from monitoring other potential threat vectors where the most insidious, long-term damage may be percolating.

The problem is most government and commercial entities just don’t have the resources required to simultaneously manage all these balls in the air. The sophistication, experience and technical skills of enterprise IT staff typically reveal limited scalability. If the people assigned to this role are not continuously focused on identifying and addressing malware, their expertise erodes rapidly. So it’s difficult for organizations to build and maintain the infrastructure and capabilities needed to effectively monitor and analyze data on hundreds of thousands of systems on a daily basis. Even among larger organizations that do have the ability to collect anomalous activity data, most are not equipped to quickly and cost effectively distinguish between benign and malicious traffic.

In a recent test scenario, random phishing attack emails containing malware-infested links and attachments were sent to 160 of the 600 employees in a federal government agency. Despite mandatory in-house training programs that cover how to recognize and respond to such social engineering exploits, 35 of the 160 targeted users clicked on the malware-infested links.

Every employee, customer and vendor interface represents a potential vulnerability for the corporate network and infrastructure, so the scope of the challenge reaches far beyond an examination of internal factors. The entire supply chain injects a scale of magnitude that exponentially expands the organization’s threat surface. In the financial services industry, for instance, the extraordinary number of interfaces maintained between banks and their account holders and business partners drastically increases the number of opportunities for bad actors to infiltrate networks.

Many organizations remain unaware of blended attacks lurking beneath the surface of the most visible or immediate threat until law enforcement notifies them of a network compromise. Agencies like the FBI use wire taps to look for command-and-control malware and monitor known data exfiltration sites for suspicious activity. Hunting capabilities empower enterprises to proactively search for and discover network anomalies before receiving a call from the authorities.

HUNTING CAPABILITIES HELP LEVEL THE PLAYING FIELD

Given the staggering amount of data now requiring protection and the broadening array of malware and tactics available to perpetrators, organizations must address this challenge from a selective perspective. Enterprises can afford to collect only the data they are able to process; the rest is useless. Comprehensive threat intelligence and analytics resources are required to identify adversary intentions and capabilities across the constantly evolving threat surface, not just in any one silo. Underlying this threat intelligence backbone, a support structure comprised of technology and process experts equipped to collect and process critical data that reveals unknown malware is essential.

In addition to response and remediation to counter the latest attacks, organizations must establish a baseline that reveals the current state of cybersecurity on their enterprise networks. Then, hunting capabilities can be used to identify all anomalous activity in order to gain a holistic view of vulnerabilities in the cyber environment so that risks can be aggressively mitigated. Unlike threat reporting services that rely on large systems and open source research designed to identify when attacks are occurring, hunting technologies proactively determine the nature and origins of attacker footprints already evident on the network.

These capabilities allow organizations to find unknown malware that cannot be identified or blocked by off-the-shelf, signature-based perimeter defenses. At least half of all cyber hunting expeditions typically uncover the kinds of stealth, targeted malware that antivirus will never detect and that presents real and imminent danger to the enterprise. Hunting methodologies sniff out smokescreens intended to mask more sophisticated social engineering exploits that give attackers ongoing access to networks for future compromise. Statistical anomalous analysis enables organizations to find the tracks that sophisticated adversaries hope will remain hidden.

“Consumers and businesses spend billions of dollars every year on antivirus software. But these programs rarely, if ever, block freshly minted computer viruses, experts say, because the virus creators move too quickly.” A group of researchers recently collected and analyzed 82 new computer viruses and put them up against more than 40 leading antivirus products. They found that the initial detection rate was less than 5 percent.

--New York Times, December 31, 2012

After anomalous activity is identified, analysis determines if it is benign or malicious, and if the latter, an intrusion forensics workup reveals all files, tools, and other indicators of compromise associated with the malware on a particular workstation. Then, by casting a wider net, it's possible to determine lateral damage—other infected machines on the enterprise network.

ENTERPRISE RISK EQUATION DEMANDS COMBINED TACTICAL AND STRATEGIC RESPONSE

The critical importance of hunting capabilities reaches beyond the tactical elements described above. As an organization improves its ability to leverage its threat intelligence support structure to gain a better understanding of adversary intentions and capabilities, visibility of the attack surface improves across all elements of people, process, policy and technology. This enables a clearer view of vulnerabilities and risk exposure across all attack surfaces, particularly with respect to where the enterprise's most critical data resides. Understanding the nature of anomalous activity and its potential impact allows enterprise stakeholders to make informed business decisions about mitigation and remediation.

The overriding tendency to focus on tactical solutions that address the most immediate problems must be balanced with longer-term strategies. The pervasive propagation of more advanced, undetectable strains of malware that bypass best-in-class cybersecurity practices coupled with an escalating number of socially engineered access points make hunting capabilities a mandatory element of the enterprise defense arsenal. Savvy perpetrators will continue to try to stay a step ahead by employing a vexing variety of attack tactics for which there are no magic bullets. But the more enterprises can stay abreast of anomalous activity, the more they will be able to keep pace with their adversaries and proactively protect vital assets.