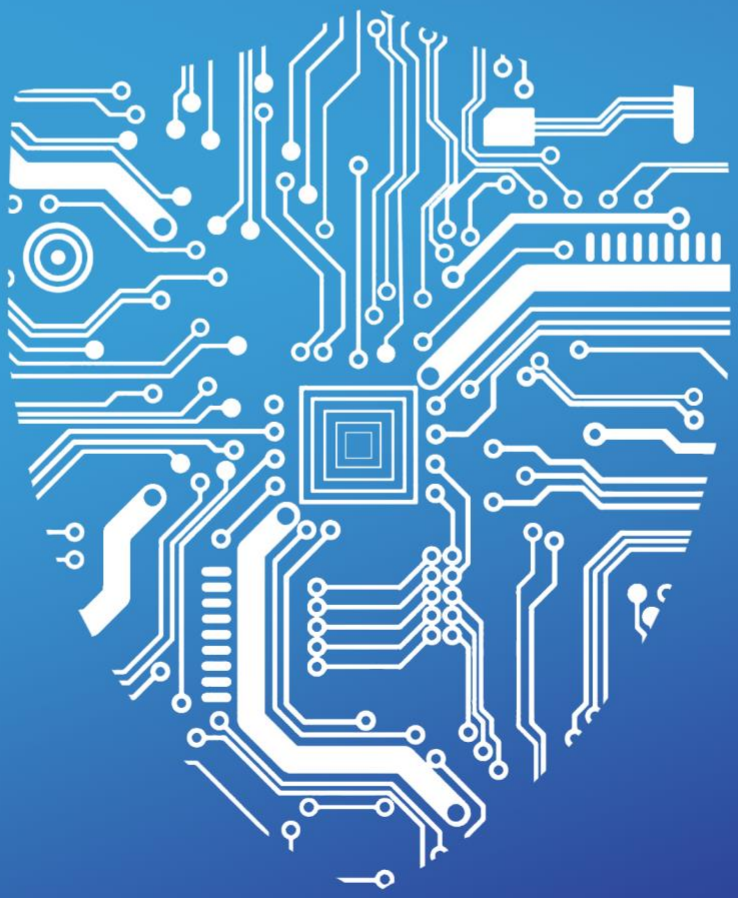
2019 TAG CYBER SECURITY ANNUAL

VOLUME 2

INTERVIEWS WITH CYBER LUMINARIES



Dr. Edward G. Amoroso

TAG cyber

Design – Miles McDonald, Alicia Amoroso, Rich Powell
Media Services – Miles McDonald, Matt Amoroso, Laura Fanelli
Finance – M&T Bank
Administration – navitend
Lead Author – Dr. Edward G. Amoroso
Researchers – Ed Amoroso, Matt Amoroso, Felix Andersen, Liam Baglivo, Ana Bolsoni, Shawn Hopkins, Miles McDonald, Ankit Parekh, Pratik Patel, Stan Quintana, Tim Steinberg
Facilities – WeWork, NYC

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

September 17, 2018

To the Reader:

Conducting and transcribing a detailed interview with an expert is harder than it looks. This is the third year we've published our questions and the corresponding answers received from various cyber security luminaries for this *TAG Cyber Security Annual, Volume 2*. While we would admit considerable remaining distance between our work and Cronkite's, we do think we are getting better. In fact, we are confident you will find this series of interviews to be the most crisp and interesting content in our three volumes – probably because our interviewees did all the work.

Our primary goal in each interview was to showcase the expert views of the *person* being interviewed. This might sound obvious, but it is often complicated by marketing and public relations teams who certainly earn their monthly paychecks. On occasion, we would submit questions and receive back cut-and-pasted responses perfectly phrased from a brochure: "Our industry-leading security solution provides superior protection of your critical assets on both premise and in the cloud." We tried to push back whenever we received anything vacuous like this.

For the most part, however, our experts – forty-five in total – were selected because their voice was simply worth hearing. Too many enterprise security teams avoid vendors like the plague, and this is a lose-lose situation. Enterprise teams lose out because they are deprived the amazing perspectives available from the cyber technology community; and the vendors lose out because they drive customers away by being too pushy about why their product would have solved the problems of Target, Sony, OPM, and Home Depot, not to mention stock fluctuations and global warming. Our interviews cut through all of that.

We recommend that you use these interviews in your day-to-day source selection or vendors and partners. If you are considering a purchase in some area of cyber security protection, then check to see if a principal from that firm is included here (or in our two previous volumes published in 2016 and 2017). Take a moment and read their words, because it will help provide for you with a sense of their purpose, belief, and intent. It's been our experience at TAG Cyber that understanding what a company and its principals *believe* is often the most important factor in determining whether their products will fit your needs.

By the way, if you are a vendor and haven't been included here – but believe this is an injustice the size of our galaxy, then please feel free to drop us an email at eamoroso@tag-cyber.com. We will do our best to set up time to review your solution offering. We cannot promise that we will make it together to second base, but we promise to try to listen to your message, and to try to understand what you and your team are about. Our experience dictates that this is the optimal means for any industry analysts to advance the community.

Wishing you nothing but the best in your cyber security work this year, enjoy this volume – and we hope it helps you save time, effort, and money.

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
Fulton Street Station on Broadway

Vulnerability Risk Lifecycle – Prediction and Validation

An Interview With
Srinivas Mukkamala
CEO
RiskSense

WHEN AN enterprise carefully examines its overall cyber risk, a so-called *attack surface* emerges, which is the set of entry points where vulnerabilities can be exploited by malicious actors. Viewing cyber risk in this way, results in the strategic objective of reducing that attack surface, generally through careful discovery of vulnerabilities combined with purposeful action designed to reduce the risk of exploits to such weak points. Predication and validation are the key activities in this regard.

RiskSense is one of the leaders in this growing area of vulnerability and cyber risk management for the enterprise. The team was instrumental in predicting WannaCry, and subsequently released useful safeguards after the initial infiltration. We recently sat down with Srinivas Mukkamala, CEO of RiskSense, to better understand how his platform addresses this area, including how his company utilizes intelligence-driven risk analytics to lead to actionable cyber security mitigation.

EA: What are the primary internal and external inputs to intelligence-driven threat analytics?
SM: Today, the best input involves collected data from vulnerability scanners. This provides a good starting point, which covers networks, applications, and databases. You then need to enrich this scanner data with threat data to truly understand what is actively being exploited. Next, users must assign criticality to those assets that have been scanned. This helps produce an overall picture of the risk of the IT infrastructure being analyzed. The resulting combination of this data supports a truly intelligently-driven threat analytics platform.

EA: How can ingested vulnerability data be normalized into an enterprise view of risk?
SM: We aggregate vulnerability data and normalize it for common terminology and data scales, mapping it to CWE, CVE, CPE, and OWASP. We then contextualize the data by correlating vulnerability relationships with multiple external threat data sources. This includes zero-day, malware feeds, exploit databases, exploit and penetration testing frameworks, dark web, and DShield. RiskSense penetration test results, as well as business criticality (e.g., asset classification and assign asset risk), deliver a complete view of the risk a given vulnerability

represents to the business. This allows us to map the results into our risk scoring model and to provide a single, credit-like risk score for every device, thus providing useful information for each business unit in an organization.

EA: Tell us about the RiskSense platform and how it addresses the attack surface.
SM: We already see that enterprises have expanded to mobile devices, networks, applications, and databases. We are also moving toward containers and IoT devices across IT and OT infrastructure. The attack surface is thus expanding rapidly and dynamically. This increases the likelihood that an attack can occur from all entry points. The RiskSense platform focuses on these attack surface entry points and allows you to incorporate vulnerability scanner data, enrich it with our 60+ threat data sources, and then factor in the criticality of your assets to derive a risk rating for each asset. The resulting risk rating drives your remediation efforts, guides your IT team on the best order for installing fixes, and ensures that you are focusing your security and IT resources wisely. The asset risk rating rolls up into department/LOB/agency risk rating, and then into an overall risk score. This score provides executives with a simple credit-like scoring framework to assess organization risk and track this over time.

EA: What is the best way to drive proper remediation once vulnerabilities have been identified?
SM: Once you have identified your vulnerabilities, you need to add threat context, basically enriching the data around these vulnerabilities, and specifically identifying which ones are exploitable in your IT infrastructure and which ones will be weaponized. Then you need to assign business criticality to each of your assets. This provides a true risk score for your specific organization, and provides prioritization on what really needs to be fixed first.

EA: Have you seen any significant trends in how your customers view and manage cyber risk?
SM: The most security mature organizations are going beyond just what to fix, and are now building out an overall security rating framework for each LOB or department or agency. They are then rolling that up into an overall cyber risk score. We call this the RiskSense Security Score (RS3). This allows organizations to track their journey in reducing risk, while keeping a continuous watch on it. These best-in-class organizations understand that their attack surface changes constantly with new devices, applications, and databases being added and removed every day. With attackers developing new attack models, they must be vigilant. Building a Threat and Vulnerability Management Program mandates a risk scoring model that guides both the security and IT Operations team which inform executives of current risk standing for an organization, this is a game changing model.