# Customer and Regulatory Requirements on IoT System Manufacturers, Result in Comparable Product Security Programs, Regardless of IoT Vertical

## A survey conducted among product security officers in automotive, industry 4.0, networking and logistics enterprises came with identical findings of product security programs, which secure IoT and edge products, against cyberattacks, adhering to customer pressure and emerging regulations

**Hod Hasharon, Israel, Bloomfield Hills, MICH** During the last 2 months, Karamba Security, a world leading product security company, conducted a series of interviews with product security officers of Fortune 500 and Global 1,000 US, European, and Japanese companies. Karamba is issuing today a report on the state of the industry.

The motivations for Product Security, as identified in the report, are clearly related to large customer demand (starting with governments and federal agencies), meeting industry-specific regulations, and drive to differentiate their IoT products thanks to strong cybersecurity features.

The survey shows that the industry is in early stages of creating the product cybersecurity officer role. Titles vary between different companies, and reporting structures are to CTO, EVP R&D, and or EVP Safety and Compliance.

On the positive side, and looking through the commonality between the different sectors and individual companies, from Fortune 100 public companies to privately owned German Mittelstand manufacturers, emerging a consistent Product Security program which incorporate governance across the organization, a secured development lifecycle practice, a set of embedded security measures and an on-going security operations that is aimed to maintain the product manufacturer visibility to security from start of production till the “End-of-life” phase of the product.

“The challenge for the Product Security Officer, as represented in these interviews, is clear” says David Barzilai, Karamba Co-Founder and Chairman “while the product resiliency to cyber-attacks is paramount for the organization, companies from all verticals interviews, and in all sizes, created similar programs to secure the device from design, to development, to production and post-production, in order to satisfy customer demands, and regulations needs”. “The more advanced companies add cybersecurity features to their products, in order to differentiate from their peers”, he added.

Karamba Security, specializing in cybersecurity technology and services for the connected devices manufacturers, is a trusted partner for this product security journey and is hosting the industry first Product Security Forum on LinkedIn.

About Karamba:

Karamba Security is the embedded security powerhouse, providing industry-leading embedded cybersecurity solutions for connected devices. Manufacturers in automotive, Industry 4.0, enterprise edge, and Industrial IoT rely on Karamba’s products and services to seamlessly protect their connected devices against Remote Code Execution (RCE) and Command Injection. After over 50 successful engagements with Fortune 100

companies, automotive OEMs, tier-1 providers and other manufacturers, connected device manufacturers trust Karamba's award-winning solutions for protecting their customers against cyberthreats.

More information is available at https://www.karambasecurity.com

Karamba Security Business Contact:

Amir Einav

+1-214-620-7320