CISO MAG

beyond cybersecurity

Volume I | Issue I | July 2017

Bug Bounty Programs
Bridging Security Gaps

GDPR is Coming
Are You Ready?

Cloud Security
Carry Your Umbrella

Demystifying Dark Web
What can Companies do?

Putting the Pedal to the Metal on a Secure Vehicle

Smarter Cities
Smarter World
Securing the Future

"With over 30+ years of experience working with enterprises globally, Symantec has gained customer confidence in India with its comprehensive Data Loss Prevention (DLP) solutions. The company has been successful in developing products on top of a unified management platform that gives customers the ability to manage policies, respond to incidents, and report on data loss risk from a single pane of glass. Symantec's information centric approach help customers gain visibility and remediate the information across all the channels - Endpoint, Network, Storage, Mobile and Cloud."

"Every endpoint is a soft target for a cyber-criminal, no matter how well it is connected to the network. Symantec provides one of the most comprehensive Endpoint Protection suites that is currently available in the market and adds advanced security features like Endpoint Detection and Response (EDR) solution to better address the changing threat landscape. The company has shifted to a signature-less prevention strategy with its Symantec Endpoint Protection 14 that refers to lesser dependence on previous generations of the product."

INDEX

EDITOR'S NOTE

With the fabric of our society now defined by the technology we use, the issue of cybersecurity has become more important than ever. Time and again, major cybersecurity breaches have shaken up the world, serving as wake-up calls for authorities and individuals to initiate measures to improve the security and stability of the cyberspace.

The threats we foresee are not expected to cease and one can only expect to uncover more calculated attacks on a wider scale. Therefore, there is a continuous need for providing unbiased and useful information to the professionals working to secure critical sectors. To provide cybersecurity experts key information and analysis to tackle critical security challenges, we have CISO MAG, an information security magazine for best practices, trends, and news.

This issue's cover story features smart cities, a topic that has been gaining attention around the world. The story discusses the importance of the security of smart cities, and explores the impending threats inherent to added technology and the need for standardization.

Move on to the Buzz section of this issue where we discuss vehicle hacking. The era of connected cars is upon us. Modern day cars are supercomputers with accelerator pedals, transmission, and brakes that can be connected to your phones. Some phone apps can even summon cars from your garage. But phones and computers can be hacked, the cars are not any less vulnerable as well.

In the Under the Spotlight section, we interview Manish Tiwari, CISO of Microsoft India, who is a result-driven cybersecurity professional responsible for various IT security initiatives in the Indian Navy and later in Microsoft India.

The magazine comprises a host of other informative features that look cybersecurity from an all-encompassing perspective—regulations, workforce development, partnerships, and much more.

Tell us what you think of this issue. If you have any suggestions, comments, or queries, please reach us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief
jay@eccouncil.org

CISO MAG
beyond cybersecurity

Volume 1 | Issue 1 | July 2017

Editorial
International Editor
Amber Pedroncelli
amber.williams@eccouncil.org

Senior Editor
Rahul Arora
rahul.arora@eccouncil.org

Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Design
Design Head and Visualizer
MSH Rabbani
rabbani@eccouncil.org

Designer
Surendra Bitti
surendra@eccouncil.org

Management
Business Head
Apoorba Kumar*
apoorba@eccouncil.org

Sales Manager
Basant Das
basant.das@eccouncil.org

Technology
Chief Information Security Officer
Subrahmanya Gupta Boda
gupta.boda@eccouncil.org

Director of Technology
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

Information Security Specialist
Manoj Kakara
manoj@eccouncil.org

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd. and printed at G97 Network Pvt. Ltd., Editor: Rahul Arora.

ADVISORY BOARD

CISO MAG is honored to have an Advisory Board that comprises some of the foremost innovators and thought leaders in the cybersecurity space. The board members provide us the strategic advice regarding the magazine general direction, including shaping our editorial content, identifying important topics and special issues, moderating discussions, and helping to create initiatives that benefit the industry at large.

Curtis is a proven technologist with over 25 years of experience in cybersecurity/defense, continuity/recovery of operations, and information governance. He is an expert in designing and implementing strategic and tactical information security architectures and best practices for organizations with a wide variety of risk postures in complex and distributed environments. Curtis has served with distinction, two sitting presidents of the United States, two chairmen of the joint chiefs of staff and the chief justice of the United States.

Curtis Levinson
Private Consultant and United States Cyber Defense Advisor to NATO

The former CISO of Cox Communications, VeriSign, and SecureIT, Phil helped transform security at GE, Alcatel, Scientific-Atlanta, Cisco, and Dell. He has influenced the privacy, cybersecurity, and IT industries for almost 30 years through his leadership and influence in policy/standards bodies and industry think tanks. He has shaped payments security on the PCI Security Standards Council Board of Advisors and FS-ISAC PPISC Steering Committee.

Phil Agcaoili
Senior Vice President, U.S. Bank, and Chief Information Security Officer, Elavon

---

Selim has over 20 years of computer and financial industry experience, and was named by the IT Security Magazine as one of the "Top 59 Most Influential Security Experts." He has published over 30 journal and conference papers and co-authored the book *Security for Mobile Networks and Platforms*. Selim has over 100 patents filed, and has previously worked with Visa as vice president of Global Information Security and headed Strategic Planning for eCommerce, Security, Manageability, Content Protection, Enterprise & Virtualization for Intel.

Selim Aissi
Chief Information Security Officer, Ellie Mae

ADVISORY BOARD

Betty has over 35 years of experience in information technology (IT), networks, application development, information security, cybersecurity, privacy, cloud services, risk management, compliance, certification and accreditation, information assurance, and other security or privacy assessments. A subject matter expert in security authorization and regulatory compliance including NIST, FedRAMP, and international regulations, her certifications include CISSP, ISSMP, CAP, CIPP/US, CIPP/G, NSA-IAM, NSA-IEM, C|CISO, and CIPM. She designed and implemented the first cybercast from the White House and led the team that won the Hammer Award for Excellence from Vice President Al Gore.

Betty Lambuth
Private Consultant

Tammy not only secures and protects Venafi, she also collaborates globally to help CIOs and CISOs fortify their strategies to defend against increasingly complex and damaging cyberattacks against the trust established by cryptographic keys and digital certificates. Tammy's professional experience, leadership, and recognized domain expertise as the CISO of Global 250 companies will help fellow CISOs defend their organizations. A veteran in information technology, she is noted by her peers to be a results-driven and passionate executive leader.

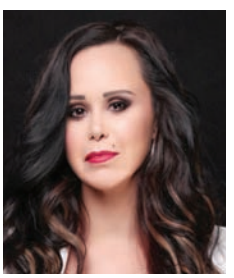
Tammy Moskites
Chief Information Officer and Chief Information Security Officer, Venafi

---

Prashant is an internationally renowned cyber law and cybersecurity expert, author and a lawyer based out of Mumbai, India. He has been awarded as the Cyber Security Lawyer of the Year-India by Financial Monthly magazine of UK (2016). He has also been awarded as Cyber Security & Cyber Law Lawyer of the Year 2014 by Indian National Bar Association.

Prashant Mali
International Cyber Law and Cybersecurity Expert

Magda calls herself a cyber feminist and a cyber evangelist. She is involved in public speaking and international conferences as a keynote speaker where she addresses industries' challenges with cybersecurity as well as diversity in the sector and the presence of women. In addition of managing her business, she acts as chief information security officer for various companies. She speaks five languages fluently, and has a PhD in Telecommunication Engineering with a subsequent specialization in cybersecurity with a CISSP certification.



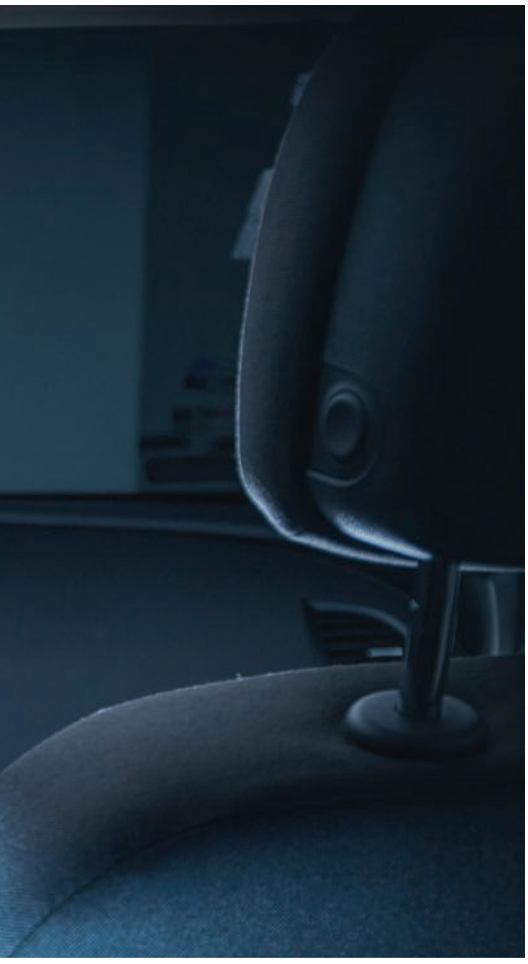
Magda Chelly
Managing Director, Responsible Cyber Pte

Sunil has over 22 years of leadership experience with renowned companies in Banking, Telecom, ITES and Manufacturing in Middle East, United States and India. He has participated in various advisory forums globally, and has published and presented several articles related to information assurance. Two of his patent application on information security is currently in consideration.

Sunil Varkey
Chief Information Security Officer, Wipro Technologies

AUTOMOTIVE CYBERSECURITY:
A NEW MARKET WITH A DISTINCT CHALLENGE

Augustin Kurian



Innovation in the automotive industry has led to a scenario where a car being manual may simply mean it has a steering wheel. Once composed of only mechanical and electrical parts, cars have now turned into complex systems that comprise sensors, microprocessors, software, and much more.

The proliferation of autonomous vehicles means that microprocessors and sensors will soon take a much more active role in driving cars. However, even before self-driving cars become commonplace, modern cars are already vulnerable to hackers via in-car technology like Wi-Fi. These "connected cars" are becoming standard. In 2015, there were around 6.5 million connected cars on the road and by 2017, the figure almost doubled to 12.5 million. According to estimates, there will be as many as a quarter billion connected vehicles on the road by 2020.

This new technology has also opened a floodgate of security threats. While you might be behind the wheel, potentially vulnerable software control your car's functions. "There is almost nothing in your car that is not mediated by a computer," said Professor Stefan Savage, Department of Computer Science, UC San Diego, while speaking to *Motherboard* magazine for a short documentary on car hacking.

Fear of car hacking has not yet penetrated the general population's psyche, as demonstrated by a 2016 Kelley Blue Book survey of drivers. The results of the survey show that among its sample size, very few drivers fear car hacking and most consider connected apps and Wi-Fi networks nice features to have.

Worries over security have also not slowed down the pace at which connectivity features continue to be rolled out due to the real benefits all this technology can bring with it. Connectivity technologies in commercial vehicles not only improve efficiency and streamline logistics, they also lower occurrences

"There is almost nothing in your car that is not mediated by a computer," said Professor Stefan Savage, Department of Computer Science, UC San Diego, while speaking to *Motherboard* magazine for a short documentary on car hacking.

of road accidents and reduce preventive maintenance costs. Incorporating connectivity technologies can also reduce 62 percent of all trucking costs, it is estimated.

A REAL THREAT

Vehicle hacking isn't just a theory or seen only in Hollywood movies. In 2016, Nissan had to shut down its proprietary app NissanConnected EV for its Leaf line-up after it was found that hackers could access the cars' climate control and other battery operated features to drain the batteries. Also, in 2015, automaker Fiat Chrysler had to issue a recall for almost 1.4 million vehicles after researchers Charlie Miller and Chris Valasek of *Wired* demonstrated a wireless hack on Jeep Grand Cherokee, taking over the controls of the dashboard, steering wheel, powertrain, and even the brakes.

Recently, WikiLeaks released documents blowing a whistle on the CIA suggesting journalist Michael Hastings's fatal car crash was triggered by a car hack. In 2013, Hastings died after the car he was driving abruptly sped up and crashed into a tree. The media has largely covered this idea as a fringe conspiracy theory, but many of the details are consistent with how a hacked car could behave.

REGULATORS, INDUSTRY RESPOND

Autonomous vehicles are no longer a pipe dream and all vehicles soon will come with smartphone connectivity embedded into their systems. Fortunately, all manufacturers prioritize the satisfaction and safety of their customers. The burgeoning field of automotive cybersecurity will grow

TAKEAWAYS FOR CISOs

In a time where cars are predicted to generate 25 gigabytes of data per hour, enterprises may need to consider connected cars as an insider threat due to their vulnerability to data theft. Cars come with connected features to pair your personal device for several purposes like hands-free driving, access to infotainment, GPS, and maps. Pairing devices like smartphones that carry sensitive data to a car's network may pose a serious threat. The data under threat can be personal or belong to an enterprise. And many times, information security heads are oblivious to the number of cloud apps in employee's device. In fact, according to a Symantec report, when most CISO/CIOs assumed employees in their organizations use up to 40 cloud apps on their devices (smartphones, tablets, laptops), in reality the number neared 1,000. The volume of exposed data is massive. CISOs need to be more vigilant, else, they may see a shift in ways data breaches occur.

To ensure the prevention of data theft from insider threats, organizations can do the following:

- Train employees on safe pairing techniques of devices and cars
- Encourage employees to charge mobile devices through cigarette lighter and not the USB
- Encourage employees to implement various security measures like installing firewall, antivirus and encryption software on employees' devices. Company-owned devices should be issued with mobile device management (MDM) software.
- In case the device is lost, there should be a way to locate and lock the device, and if necessary, the device should be implanted with a kill switch.

in partnership with regulatory and compliance bodies, original equipment manufacturers (OEMs), technology companies, insurance companies, and other stakeholders pressing for safe and secure architecture. Connected and autonomous automobiles are dynamic threat environments and numerous patrons are collaborating with groups like the newly formed Auto-ISAC, to sketch guidelines, standardizations, and best practices. These bodies endorse integration of cybersecurity into the entire lifecycle of a vehicle – from concept to production, maintenance, and decommission.

Even governments are taking notice of this. Earlier this January, a bipartisan bill titled 'Security and Privacy of Your (SPY) Car Study of 2017' was introduced in the United States focusing on the cybersecurity of automobiles. The bill mandated that the National Highway Traffic Safety Administration create appropriate cybersecurity standards for vehicles. Other nodal agencies mentioned in the bill were the Department of Defense, National Institutes of Standards and Technology, and the Federal Trade Commission, among others. The bill stressed the importance of isolation measures to separate critical software from trivial programs and take measures to detect anomalous codes.

The European Union Agency for Network and Information Security (ENISA) has also envisaged similar scenarios and come up with a report on 'Cyber Security Resilience of Smart Cars.'

The European Union Agency for Network and Information Security (ENISA) has also envisaged similar scenarios and come up with a report on 'Cyber Security Resilience of Smart Cars.'

GROWING TECH, BROADER SAFETY NET

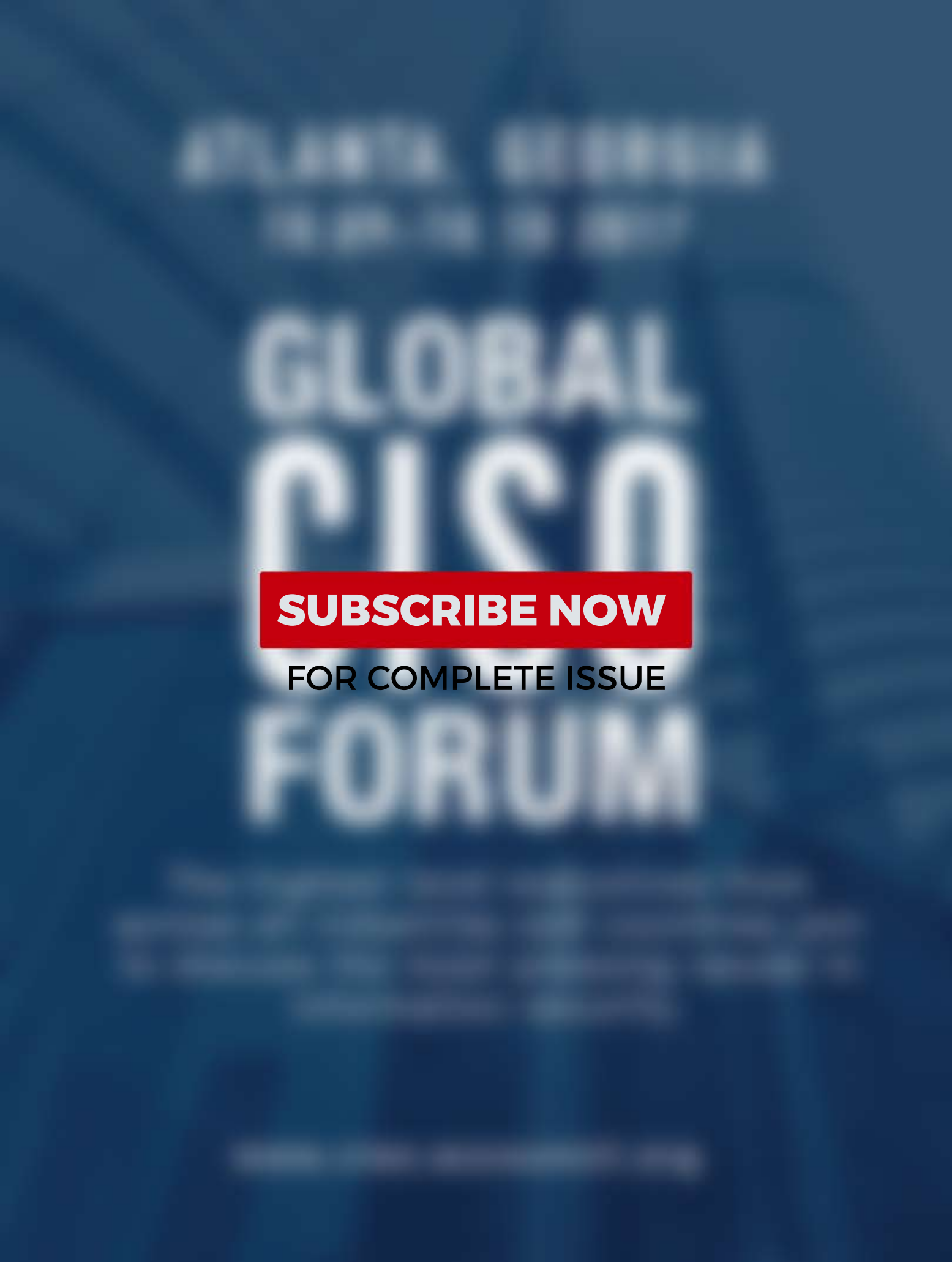
Security cannot be an afterthought—it must be integral throughout the design process. Automotive cybersecurity is a new emerging market. According to report titled 'Automotive Cyber Security - Global Forecast to 2021,' the global automotive cybersecurity market is projected to grow at a compound annual growth rate (CAGR) of 13.2 percent by 2021, to reach a market size of $31.8 million by 2021.

A sizeable number of private firms are also venturing into automotive

cybersecurity. Israeli startup Karamba Security unveiled security systems for connected cars that prevent hackers from running any malicious code on the car system like lane assist, infotainment, and GPS tracking. Another startup working in the same field is Argus Cyber Security. Argus helps car manufacturers, their Tier 1 suppliers, and aftermarket connectivity providers protect connected cars and commercial vehicles from hacking.

This is the Internet of Things (IoT) era and cars are no longer basic modes of transportation. Connected cars could be a new and refreshing use of big data and a business model worth leveraging as insights from these data can be monetized. A McKinsey report states that, "Once autonomous driving and car connectivity combine, customers might be offered mobility services in exchange for watching targeted advertisements, providing product feedback, or making purchases while in the car." Businesses in the future might also leverage these systems to offer free rides to stores to retain customer loyalty.

The initial architecture of car networks is now almost 30 years old and was devised for various reasons, but security was not one of them. The systems were designed without an inkling that vehicles could be hacked, but it's not too late. It's time for cybersecurity professionals to step in and do what they do best– clean up the tech to avert disaster.


GLOBAL
CISO
FORUM
SUBSCRIBE NOW
FOR COMPLETE ISSUE