CISO MAG

beyond cybersecurity

Volume 3 | Issue 1 | January 2019

2019

DAWN OF A NEW ERA

INDEX

Volume 3 | Issue 1

14
BUZZ
Cybersecurity Predictions:
2019 and Beyond

26
COVER STORY
Dawn of a New Era

52
INSIGHT
The Bandwagon Effect

60
COLLABORATIONS
InfoSec
Partnerships

72
IN THE NEWS
Top Stories from
the Cybersecurity World

80
IN THE HOTSEAT
High-Profile Appointments in the
Cybersecurity World

86
KICKSTARTERS
Startups Making Waves in the
Cybersecurity World

EDITOR'S NOTE

It may be argued that year 2018 is the kind of year information security sector wanted, or perhaps needed, after the mayhem of 2017. While 2018 also had its share of gruesome and frequent cyber incidents, the brighter moments weren't few and far between. One of the main reasons behind 2018 being a little "sober" in comparison of 2017 was the significant amount of legislative activities from different nations.

It all started with Singapore passing the Cybersecurity Bill followed by implementation of General Data Protection Regulation in Europe and Data Breach Notification Act of 2018 in the United States. Other countries also showed their concerns toward cyber breaches and announced or began framing stringent regulations to address the issue. While these regulations did ruffle some feathers and created a bit of stir, experts believe there are long-term gains attached to them. Our Cover Story looks back at 2018 in detail and discusses the chaos and glimmers of hope the year brought with it.

There is no doubt that the future of cybersecurity will continue to be tested in 2019. Our Buzz section discusses the trends and activities most likely to affect public and private sector in 2019. The Insight section of this issue addresses the Bandwagon Effect in cybersecurity and its drawback.

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

CISO MAG
beyond cybersecurity

Volume 3 | Issue 1
January 2019

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

Senior Editor
Rahul Arora
rahul.arora@eccouncil.org

Senior Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Media and Design
Media Director
Saba Mohammad
saba.mohammad@eccouncil.org

Designer
Suresh CH
suresh.ch@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

Senior Director,
Compliance & Governance
Cherylann Vanderhide
cherylann@eccouncil.org

Marketing & Sales
General Manager
Meghana Vyas
meghana.vyas@eccouncil.org

Marketing and Business Development Officer
Riddhi Chandra
riddhi.c@eccouncil.org

Sales Manager - North America
Jessica Johnson
jessica.johnson@eccouncil.org

Technology
Director of Technology
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Rahul Arora.
The publishers regret that they cannot accept liability for errors & omissions contained in this publication, howsoever caused. The opinion & views contained in this publication are not necessarily those of the publisher. Readers are advised to seek specialist advice before acting on the information contained in the publication which is provided for general use & may not be appropriate for the readers' particular circumstances. The ownership of trade marks is acknowledged. No part of this publication or any part of the contents thereof may be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.

Volume 3 | Issue 1

COVER STORY

Dawn of a New Era

-Augustin Kurain & Rudra Srinivas

27

CISO MAG | January 2019

Volume 3 | Issue 1

COVER STORY

The WannaCry ransomware attack of 2017 was a bit like an old wine in a new bottle, but that doesn't mean we didn't get a little drunk. When WannaCry, the NSA's Eternal Blue spying tool, was stolen and unleashed to infect the world, it lived up to its name. WannaCry remains one of the largest, most successful ransomware campaigns to have ever been executed. But that is a story of 2017. Compared to the year in which magnum opus of the Lazarus hacker group made us weep, 2018 may appear to be rather sober. However, 2018 had its share of tear-inducing moments as well as some soaring triumphs of regulation. The year saw a continuation of the trend of cryptocurrency hacks, perhaps putting a damper on the enthusiasm for the future technology, as well as new laws designed to protect consumers around the world. Let's take a look back at the year that was 2018.

Breaches, attacks, and vulnerabilities

The information security of India was called into question after *The Tribune*, one of the country's largest newspapers, reported a complete lack of security in India's UIDAI (Unique Identification Authority of India) program in early January. The program was supposed to bring the country's 1.3 billion population onto a digital platform with unique identity numbers. *The Tribune* found that agents were selling gateway tools and accessing login credentials for less than $10; anyone could purchase the address, postal code (PIN), photo, phone number and email of any citizen as long as the Aadhaar number of the person is provided. Moreover, the investigative journalists found that for another five dollars, they could they could obtain a printed Aadhaar card of any individual. This security blunder was easily the largest of 2018 as far as number of victims was concerned, as it involved the details of nearly $1.1 billion people.

While the UIDAI fiasco might have been the largest as far as the numbers, the most sensational incident of 2018 was undoubtedly the Facebook situation, which in early March landed the founder in court. It emerged that Facebook was sharing the personal information of 50 million of its users with data firm Cambridge Analytica, though Cambridge Analytica argued that it was 30 million. The social networking giant eventually notified 87 million users that their data may have been shared. Later in March, Under Armour's MyFitnessPal app was breached due to a notoriously weak password hashing function called SHA-1, exposing the usernames, email addresses, and hashed passwords of nearly 150 million users.

The biggest major attack in April was Panera Bread. In a post, KerbsOnSecurity pointed out that the American chain of bakery-cafe fast casual restaurants has leaked the data of millions of customers including names, email and physical addresses, birthdays, and the last four digits of the customer's credit card numbers. It said, "the website let's anyone search by a variety of customer attributes, including phone number, email address, physical address or loyalty account number." The