CISO MAG

beyond cybersecurity

Volume 4 | Issue 07 | July 2020

CYBERSECURITY IN THE TIME OF A PANDEMIC

THE NEW NORMAL

CISO MAG
beyond cybersecurity

Volume 4 | Issue 7
July 2020

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

Principal Editor
Brian Pereira
brian.p@eccouncil.org

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

Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Technical Writer
Mihir Bagwe
mihir.b@eccouncil.org

Feature Writer
Pooja Tikekar
pooja.v@eccouncil.org

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

UI/UX Designer
Rajashakher Intha
rajashakher.i@eccouncil.org

Sr. Graphics Designer
Sameer Surve
sameer.s@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

Deputy Business Head
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

Head of Marketing
Deepali Mistry
deepali.m@eccouncil.org

Marketing Manager
Riddhi Chandra
riddhi.c@eccouncil.org

Digital Marketing Manager
Jiten Waghela
jiten.w@eccouncil.org

International Sponsorship Manager
Mir Ali Asgher Abedi
mir.ali@eccouncil.org

Publishing Sales Manager
Taruna Bose
taruna.b@eccouncil.org

Publishing Sales Manager
Vaishali Jain
vaishali.j@eccouncil.org

Executive – Marketing and Operations
Munazza Khan
munazza.k@eccouncil.org

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

Image credits: Shutterstock
Illustrations, Cover & Layouts by: Rajashakher Intha

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Brian Pereira.
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 & July 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 July be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.

EDITOR'S NOTE

THE CISO MUST DO DUE DILIGENCE ON SECURITY

The past three months have witnessed a flurry of activity in the corporate world. To reduce the impact of the deadly COVID-19 virus, organizations relocated their workforce and adopted a remote operating model. Employees reached for new technologies and collaboration apps – whether they were approved by their corporations or not. As if that wasn't enough, businesses were forced to remodel and accelerate cloud migrations. And this has not only increased operational complexity but also broadened the threat landscape.

We know that hasty decisions can lead to costly mistakes. And therefore, one needs to take a structured approach and make informed decisions, which means doing due diligence.

That applies to cloud migration and security as well.

Our Editorial team thought this is the right time to bring out an issue on the impact of COVID-19 on the cybersecurity world and information security professionals. So, they went about curating a set of articles on this theme that could help CISOs navigate this time.
Be sure to read our Cover Story titled "Need-Based Evaluation of Cloud Services in the Wake of COVID-19," written by **Stan Mierzwa,** Director, Kean University Center for Cybersecurity. He writes about the pressure that organizations face in the wake of COVID-19 to hurry cloud migrations. Organizations that are using legacy applications have started evaluating cloud services and cloud service providers. He cautions organizations to do due diligence on cloud security using the tools and resources cited in his article.

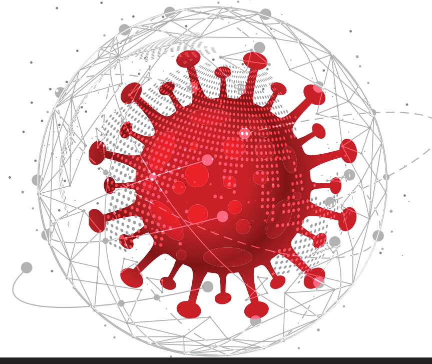
Eric Jeffery, Sr. Managing Consultant and Solutions Architect, IBM Security, echoes this sentiment in his article "Cybersecurity After COVID-19" in Knowledge Hub. He advises CISOs to have a clear understanding of the technologies and processes in place and make the necessary adjustments after COVID-19 to prevent attackers from succeeding in perpetuity.

A related article to read in this issue is "Cybersecurity – Top 5 lessons learned from COVID-19," written by **Hemanta Swain**, VP & Chief Information Security Officer at Tivo Corp. He draws interesting comparisons between the pandemic and his infosec professional life.

We hope you are safe and well.

Please write to us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief



INDEX

A NOTE OF CAUTION ON THE DIGITAL DOCUMENT REVOLUTION

- Ian Lancaster,
Founder and former Managing Director of Reconnaissance International
and lead author and editor of ‘Physical to Digital: A Revolution in Document Security’

A revolution is underway in the secured document field. Society is migrating from using physical secured documents, such as banknotes and identity cards, to the use of smartphones and electronic payment cards for financial transactions and as carriers of our identity credentials.

The COVID-19 crisis has thrown this trend more sharply into focus in relation to payments. In just one week, cash usage halved in the UK and a similar story is playing out around the world as more people turn to contactless payments to minimize the spread of the virus. Whether this is a temporary measure while the virus is active or another nail in the coffin of cash, remains to be seen.

In the minds of many people, this transition from physical to digital is inevitable, unstoppable, and irrevocable, even though cash is still used for most retail purchases globally (COVID-19 influence aside).

On the other hand, certain physical documents like passports are still required to enter a territory. Nonetheless, this transition is inevitable, so there is a need to consider the impact and implications of this change.

These considerations are the driving force behind Reconnaissance International's new White Paper, *"Physical to Digital: A Revolution in Document Security,"* which looks at the implications of the current digital revolution in the areas of financial transactions and ID document security. The publication contrasts more than 1,000 years experience in printing and examining security documents with the 30 years of digital experience, and the use of smartphones in what has previously been the domain of secured printed documents.

In simple terms, is it a revolution that leaves us and our data safe? We are moving from a world in which people can examine and inspect a document to check its legitimacy (in order to be confident it can be trusted), to one in which we have to trust that a device, such as our smartphone, is doing what we think it's doing, that the data it's using is accurate and secure, and the decision it makes – or leads us to make – is correct and appropriate.

Are we right to invest this much trust in these new methods of making payments and showing our identity? Or should we pay heed to the view that, in failing to question the algorithms that are doing this work for us, we open the door to cyber criminals?

In examining the transition in security documents from the physical to the digital, our White Paper considers:

- How far has it gone and what is its future?
- What are its implications and – crucially – how safe is the data held and used in the digital world?
- Are we merely users of these systems, or is there a role for us in ensuring that they and the data they use are secure? What might that role be?
- Is anything needed to enhance the safety and security of these digital methods and if so, what?

The Current Landscape

The use of digital technologies has some way to go before replacing cash – most people in most countries continue to rely on cash for retail transactions. Similarly, when it comes to ID documents (like passports), digital technologies, while attractive, remain for the time being some way short of being ubiquitous. It's clear that physical banknotes and ID credentials remain the norm – but why?

Physical documents are tangible, familiar, and with security and authentication features built in. Moreover, a key driver for specifiers and designers – honed over these 1,000 years of experience – is security and document protection. In this physical world, professional document examiners develop a sixth sense, a feeling for the document which comes with familiarity and practice.

The result is reflected in the low counterfeiting levels for banknotes and passports; for example, 0.003% of euro banknotes in circulation and 2% of passports worldwide. This compares to, say, the World Health Organization's estimate that 10% of medicines worldwide are fake.

As digital methods become more common, we need to question whether they match the security and detection built into the physical document world. If not, how can they be improved? Should we abandon the use of human inspection and, if not, how do we combine the best of both worlds?

These questions become more pertinent when we consider the significant number of data breach-

[illegible]