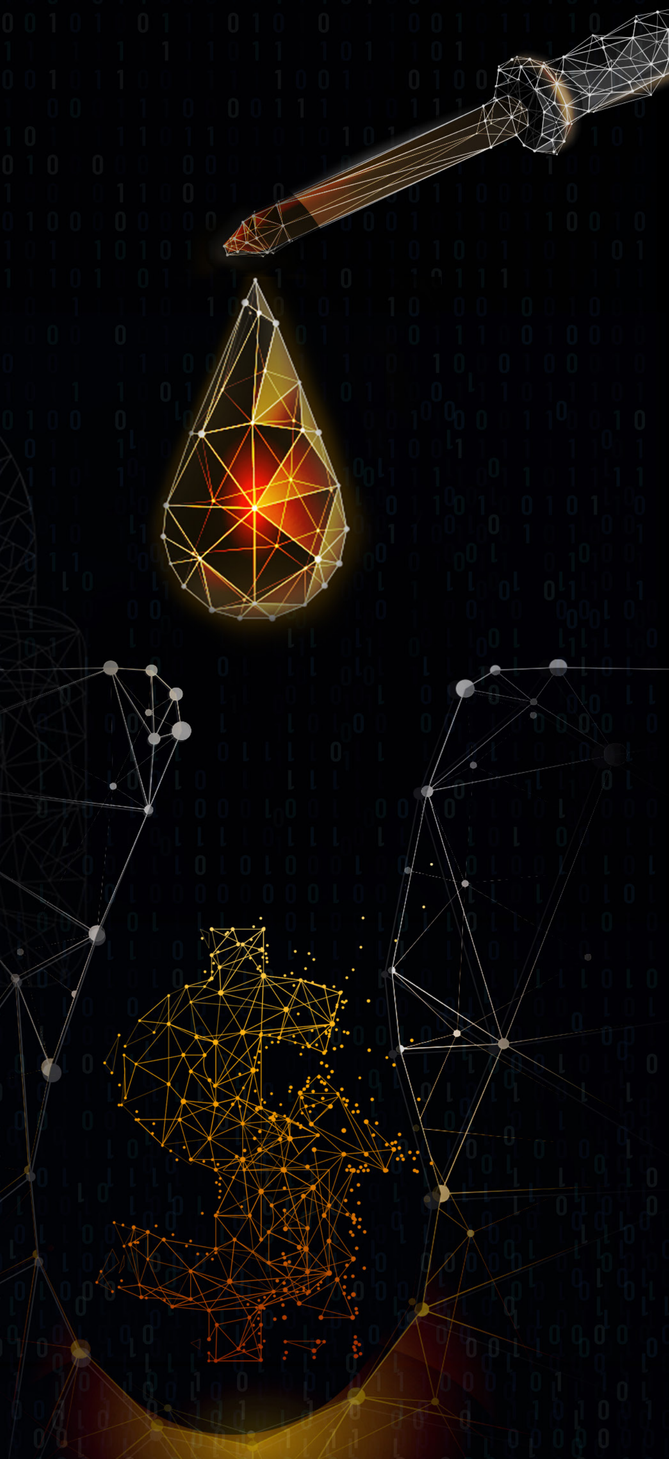
CISO MAG
beyond cybersecurity

Volume 4 | Issue 09 | September 2020



SECURING DATA

THE NEW OIL OF THE DIGITAL ECONOMY

An EC-Council initiative

We'd like you to meet...

Hailey

Reduce Cost & Complexity

Unleash a unique and powerful combination of natural language processing and machine learning to significantly reduce the cost of compliance.

Accelerate Alignment

Enter new markets, demonstrate compliance and ensure control effectiveness faster than ever before – reduce months of effort to seconds.

Gain Better Insights

Gain better insights with market intelligence tailored to your risks and obligations – real time, relevant and enhanced with the power of social.

Artificial Intelligence
for Risk Management & Compliance

6clicks™
Delivering Trust

CISO MAG

MARKET TRENDS REPORT ON
ENDPOINT SECURITY

COMING SOON

The Highest Level of Security on the Go

Military Grade Security * Affordable * Easy to Deploy / Manage * Made in the U.S.

SPYRUS Solutions provides the strongest protection of data in motion, at rest and in use. For 20+ years, SPYRUS encryption, Multi-factor Authentication, and digital signature and content products have enabled customers to meet stringent Public and Private regulatory data protection requirements with the highest level of confidence. FIPS 140-2 Level 3 validated, anti-tamper USB and microSD tokens offer protection for any after market computing / IoT device; our Rosetta security chip provides OEM partners with equivalent onboard security; and our DevicePatrol™ platform enforces enterprise policies to all Rosetta protected user or unattended devices.

www.spyrus.com

SECURED BY SPYRUS

CISO
MAG
beyond cybersecurity

Volume 4 | Issue 9
September 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

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

SECURITY IS PARAMOUNT FOR CUSTOMER DATA

As the U.S. elections draw near, I am reminded of the Facebook-Cambridge Analytica data breach reported in early 2018. Without consent, personal data of millions of Facebook users was allegedly harvested and sold to Cambridge Analytica for political advertising. The massive data scandal eroded Facebook's reputation, and users closed their accounts and abandoned the social media giant with disdain. Remember the #DeleteFacebook online movement? That one incident changed the world and became a talking point in data privacy discussions.

If this incident were to be repeated today, the organizations involved could be heavily penalized with stiff fines imposed by GDPR, CCPA, and other regulatory norms.

But our story is not about fines and loss of reputation.

Organizations are responsible for protecting customer data, personally identifiable information, confidential data, intellectual property, and transactional data. Data sovereignty and data residency are on the compliance checklist.

Governments, CISOs, and CDOs (Chief Data Officers) need to have a holistic approach and ensure Data Security, Data Governance, and Data Integrity through stringent compliance and policies. They must ensure that data access is strictly on a need-to-have basis. These are the tenets for customer trust, loyalty, and the reputation of an organization.

With enterprise infrastructure increasingly moving to the cloud, an organization's data is in transit through public networks. It goes to the cloud for processing and is momentarily held in storage buckets or data lakes; it could go to a partner's network or database. It is likely to transgress borders at lightning speed and go to servers in other regions and availability zones (a matter of great concern for government and regulators). It then comes back to storage/a database and finally ends up in archival or offline backups. So, it is necessary to secure data wherever it exists – throughout the data life cycle.

It is common for enterprises to host their infrastructure in hybrid, multi-cloud environments. In this scenario, it is vital to implement a singular data protection strategy across an enterprise, on-premise, and hybrid and multi-cloud environments.

This issue of *CISO MAG* includes our third Market Trends report for the year on Data Security. The aggregated findings in the report are confirmed by 231 survey respondents and validated by industry experts.

Our latest report observes that 80.95% of respondents want to protect Contact/Identity information, and 77.92%are particular about Financial/Banking data. Secondary importance is given to Medical Records/EHR, location data, and Biometric data.

Please read the full report on page 54 for other revealing data points and insights.

Our next Market Trends report will be released in December, focusing on **Endpoint Security.**

We hope you enjoy reading all the other articles in this issue as well.

Please write to us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief

INDEX

ENTERPRISE

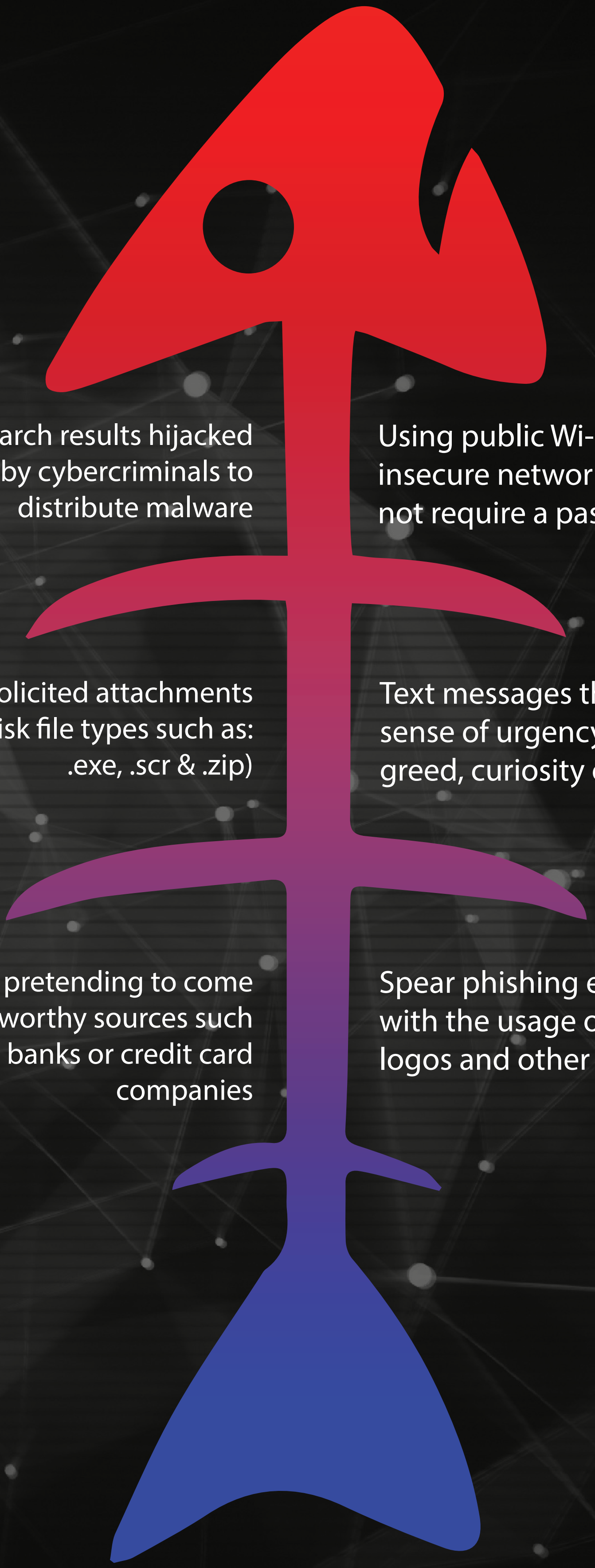
CISO MAG
beyond cybersecurity
MARKET TRENDS REPORT ON
DATA SECURITY

If you aren’t Phishing your staff, somebody else might be!

OHPHISH

Fortifying Front Lines

Click for your free demo!



Web search results hijacked by cybercriminals to distribute malware

Using public Wi-Fi especially insecure networks that do not require a password

Unsolicited attachments (high-risk file types such as: .exe, .scr & .zip)

Text messages that create a sense of urgency, panic, greed, curiosity or fear

Emails pretending to come from trustworthy sources such as banks or credit card companies

Spear phishing emails with the usage of corporate logos and other identifiers

Ways You Could Get Hooked

THE 2ND EDITION

AFRICA CISO FORUM

AN EC-Council INITIATIVE

#HyperCyberSec
#CISOMAGLIVE

Join us, where the **African Infosec Community** will meet. And witness **gripping discussions**, **engrossing keynote sessions** and **engaging innovation addresses**.

17th September, 2020
Nigeria (9:55 AM) - South Africa (10:55 AM)
Kenya (11:55 AM) - Egypt (10:55 AM)

REGISTER NOW

Engage with Africa's Top Infosec Leaders

Prasanna Kumar Burri
Group CISO
Dangote Industries Limited

Harrison Nnaji
CISO
First Bank Nigeria

Justin Williams
Executive: Group Information Security,
MTN Group

Abeer Khedr
Information Security Director
National Bank of Egypt

Kerissa Varma
CISO
Old Mutual Limited

Daniel O. Adaramola
CISO
Unity Bank

Zaid Parak
Group CISO
Discovery Limited

Yusuph Kileo
Cybersecurity & Digital Forensics Expert

Hassan Hafez
Head of IT,
Total Egypt

300+ Infosec Leaders

100+ Top Companies

Individuals

Corporates

Startups

Government

Products

Academia

SPECIAL FEATURES

KEY QUESTIONS FOR IMPLEMENTING STRONG SECURITY AND COMPLIANCE PROGRAMS

Jason Taule
Vice President of Standards & CISO
HITRUST

To arrive at the right answers, one first needs to ask the right questions! CISOs who discover that their actions do not generate the desired results to strengthen security and compliance postures may not be asking the right questions. Effectively managing data, information risk, and compliance is complex and ever-changing. There are many components and considerations in developing and implementing a robust program that encompasses and integrates all the elements needed to manage risk and achieve one's compliance objectives effectively. A critical component is making sure to ask the right questions of the right people.

The right questions include those that CISOs should ask themselves as well as the management team, the operations team, and other key stakeholders, including the Board of Directors. CISOs who come up with the questions on their own will likely tailor the questions to their situation and environment — often driven by functional and operational priorities that may not directly line up with the top-line business objectives. More specifically, an ad-hoc approach usually overlooks some of the core questions that matter in establishing a strong security and compliance posture.

Answer the Right Questions to Drive Business Results

By collaborating with people from across the organization and asking questions focused on risks and controls tied directly back to the business, CISOs can drive decisions that truly get at what the organization needs to achieve the security and compliance postures the business is seeking. This, in turn, leads to an action plan to produce the desired business results.

The ad-hoc approach perpetuates managing the security and compliance program in a reactive fashion — where the focus is only on the immediate situation at hand. How should CISOs avoid situations where they have to ask themselves, "Where did I fail the business?" They can do this by taking a results-driven, proactive approach adopted by others in their industry. They can work with internal stakeholders to adopt a set of questions that demonstrate how to get to the "why" behind their security and compliance programs.

The Pitfalls of Creating Risk Profiles Based Purely on the Technical Environment

A key responsibility for every CISO is to seek the necessary information to understand their company's security and compliance risks. The resulting risk profile can then be translated into recommendations and options that the internal security team and executive team members can understand, throw their support behind, and take action. Ultimately, it's about the action; and action must have a purpose more significant than the technical elements that technology leaders lean on.

Early in a CISO's career, it may seem that the questions to ask to find such information must be explicitly created for the technical environment that's being secured and the business environment is supported. This, however, could lead to many issues:

- Misaligned or missing questions
- Baited or ill-timed questions
- Yes/no questions that do not provide context
- Questions that do not go deep enough or don't connect to tell the full story
- Questions that do not drive an understanding to get buy-in to act from the business

Instead, what is needed is a list of questions, in the right order, and a projection of what the answers could be, might be, and should be. Projecting the answers helps make sure the questions are on target and presented in an order that will elicit contextualized thinking. This may also result in the need to re-visit the questions once previous assumptions are confirmed or refuted.

Another critical facet is deciding when to ask the questions of each stakeholder. The results of each interview could influence the questions of subsequent discussions. So, the order in which the CISO connects with the stakeholders is critical. And after collecting the answers, the CISO needs to validate the information and investigate unforeseen responses to find out what is reasonable and if any these provide incorrect information.