CISO MAG

beyond cybersecurity

Volume 5 | Issue 07 | July 2021

4 YEARS ANNIVERSARY

THE INTERVIEW ISSUE

Spotify

Listen Now

Supply Chain Attacks and Vulnerability Disclosures

How should governments, businesses, and the industry respond to the series of cyberattacks on supply chains? Will increased regulation and Responsible Vulnerability Disclosure help? Listen to what Ran Nahmias, Co-Founder and Chief Business Officer at Cyberpion, has to say.

PLAY

Spotify

EPISODE #7

CISO Culture Is All About Focusing on the Negatives

Spotify

EPISODE #6

How Insurance Fraud is Evolving (and Anti-fraud Measures)

Spotify

PLAYLIST

CISO MAG

Playlist description

Created by **Podcast Channel**

PLAY

Download

TITLE

EPISODE #1	21:40
EPISODE #2	20:45
EPISODE #3	20:41
EPISODE #4	25:32
EPISODE #5	23:13
EPISODE #6	21:44
EPISODE #7	20:45

CISO MAG

beyond cybersecurity

Spotify

Listen Now

How Do We Help Small and Medium Businesses with Cybersecurity?

In this episode, Brian Pereira, Editor-in-Chief, CISO MAG interviews Chris Roberts, Researcher, Hacker, and CISO, to discuss the impact of cyberattacks on small and medium businesses.

PLAY

LISTEN
LATEST CYBI
TRENDS AND
POPULAR
LEADERS O

Spotify

EPISODE #9

Protecting 5G Networks from Sophisticated Cyberattacks

Spotify

EPISODE #3

How Zoom is Enhancing Security and Evolving its Product

Spotify

Listen to the podcasts exclusively on

Spotify

Spotify

Intel Labs' Breakthrough Research on Data Privacy and Encryption Technologies

In this episode, researchers from Intel Labs in the U.S. explain how Federated Learning and Homomorphic Encryption is driving new applications that require secure data sharing and data privacy.

PLAY

Spotify

Digitization and Cybersecurity in Fourth Industrial Revolution

Takashi Amano, General Manager, Cyber Security Center, Toshiba Corporation talks about the limitations of conventional corporate security systems in the manufacturing domain, and the steps his company has taken to protect intellectual property. In this episode, he is joined by **Kumar Ritesh**, Founder and CEO, CYFIRMA.

PLAY

Listen to the podcasts exclusively on

Spotify

Spotify

EPISODE #2

Digitization and Cybersecurity in Fourth Industrial Revolution

01:12 20:45

Spotify

EPISODE #11

Supply Chain Attacks and Vulnerability Disclosures

01:12 20:41

PODCAST

Spotify

PLAYLIST

CISO MAG

Playlist description

Created by **Podcast Channel**

PLAY

Download

TO THE
ERSECURITY
INSIGHTS BY
INDUSTRY
ON THE GO.

Spotify

Listen Now

Protecting 5G Networks from Sophisticated Cyberattacks

In November 2019, the U.K. government introduced the Telecommunications Security Bill which imposes harsher fines for operators who fail to protect their networks and subscribers.

PLAY

01:12 20:42

TITLE	
EPISODE #8	21:40
EPISODE #9	20:45
EPISODE #10	20:41
EPISODE #11	20:41
EPISODE #12	23:13
EPISODE #13	21:44
EPISODE #14	20:45

Spotify

EPISODE #1

How Digital Risk Management (DRM) is Changing During the Pandemic

01:12 21:40

Spotify

EPISODE #10

The Case for Virtual Cybersecurity

01:12 04:42

Spotify

Listen Now

CISO Culture is All About Focusing on the Negatives

In this episode, Adam Palmer, Chief Cybersecurity Strategist, Tenable, explains cybersecurity metrics and the CISO culture of focusing on the negatives.

PLAY

01:12 20:42

codered
FROM EC COUNCIL

EC-Council

OUR **BEST RESOURCE** TO UPSKILL YOUR **CYBERSECURITY TEAM'S PRODUCTIVITY**

Upskill your IT teams with custom curriculum mapping, dedicated course development that targets your organization's needs, and deep analytics that always puts you in the driving seat of your team's training.

BROWSE COURSES IN YOUR FAVORITE CATEGORIES

CUSTOMIZATION PUSHED TO THE LIMIT

Your teams' needs are at the heart of every enterprise offering we provide so you can see real relevant results. Fast!

Create custom course Bundles

Assign users

Track learning through dashboard

Custom Curriculum Mapping

Our top program architects help you assess the skill gaps in your teams, and then customize a learning path that addresses those gaps.

Custom Course Development

We can even work with our industry-leading authors to create special programs just for your team.

Assign Personalized Learning Paths through bundles

You can also design and assign different learning paths to different groups within your organization to target specific knowledge gaps.

Upskill your team with **CodeRed** for Enterprise

Cyber Talks

Worried About Rising **IoT Attacks** in the **Healthcare Sector?**

Join Expert-Led Webinar on

IoT Based Attacks in the Healthcare Industry:

Do You Know How to Respond?

| 15th July 2021

| 7.30 pm IST / 8.00 am MST / 9.00 am CDT

Register Now!

Key Issues to be Addressed:

1. **How is IoT used in the healthcare industry?**
2. **What are the major impacts of IoT in the healthcare industry?**
3. **Types of IoT-based attacks on healthcare devices**
4. **How to respond to such attacks.**

Moderator:

Amol Kodag
Engineering Director – R&D, Medtronic.
Heading Cardiovascular Portfolio
at Medtronic Engineering and Innovation Center (MEIC)

Panelists:

Scott E. Augenbaum
Retired FBI Supervisory Special Agent / Cyber Division

Ricoh Danielson
Executive Cyber Security Advisor of Incident Response and
Digital Forensics at 1st Responder LLC – A Cyber Security Firm

More Details

Volume 5 | Issue 07
July 2021

President & CEO
Jay Bavisi

Editorial
Editor-in-Chief
Brian Pereira*
brian.p@eccouncil.org

Assistant Editor
Augustin Kurian
augustin.k@eccouncil.org

Sr. Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Sr. Technical Writer
Mihir Bagwe
mihir.b@eccouncil.org

Sub Editor
Pooja Tikekar
pooja.v@eccouncil.org

Management
Senior Vice President
Karan Henrik
karan.henrik@eccouncil.org

General Manager - Marketing
Seema Bhatia
seema.b@eccouncil.org

Senior Director
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

Head - Research & Content
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

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

Manager - Digital Marketing
Rajashakher Intha
rajashakher.i@eccouncil.org

Asst. Manager Visualizer cum Graphic Designer
Jeevana Rao Jinaga
jeevana.r@eccouncil.org

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

Image credits: Shutterstock & Freepik
Illustrations, Survey Design, Cover & Layouts by: Jeevana Rao Jinaga

* Responsible for selection of news under PRB Act. Printed & Published by Brian Pereira, E-Commerce Consultants Pvt. Ltd.,
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.

FIGHTING BACK (WE'VE HAD ENOUGH!)

Brian Pereira
Editor-in-Chief

The Colonial Pipeline attack on May 7 was a watershed moment in the universal fight against ransomware attacks. It was the first incident in which the ransom paid to attackers was recovered. The attack on Colonial impacted the fuel supply chain, leading to a temporary fuel shortage along the Northeast coast of the U.S. The pressure was building for Colonial Pipeline and their CEO, Joseph Blount, had to make a difficult decision – paying up. In an interview with the *Wall Street Journal,* Blount acknowledged he authorized the ransom payment of 75 Bitcoin, which is approximately $4.4 million. A few weeks later, the Department of Justice and the FBI announced that they recovered most of the ransomware amount.

In his blog post dated June 16, Brian Krebs, Editor of **KrebsOnSecurity**, reported that the Ukraine Cyber Police arrested six people from the CLOP ransomware group. The gang reportedly extorted more than half a billion dollars from victims.

Ransomware attacks are now an everyday occurrence. A report from Cybersecurity Ventures estimated a ransomware attack on businesses every 11 seconds in 2021.

While there are numerous debates about whether impacted companies should be paying the ransom, we could soon have legislation for this. Last year, the Department of the Treasury's Office of Foreign Assets Control (OFAC) published an advisory informing the public that the payment of ransom demanded by cybercriminals may be a violation of U.S. law.

For sure, there will be more ransomware attacks in the coming months. The adversaries see this as a lucrative opportunity, more so now, when the pandemic has office workers at home, with weak security on their home networks. Ransomware gangs are getting more organized with affiliate programs. They now offer Ransomware-as-a-Service – case in point, the DarkSide ransomware group that brought Colonial Pipeline to its knees. Read more about this in "The Vulnerabilities that Open the Door to Ransomware" on page 68.

So, are we just going to sit around and watch? And become the next victim?

Isn't it time we did something about it?

The fight against ransomware attacks goes beyond private organizations, as even governments and critical infrastructure are being attacked.

Immediately after the Colonial Pipeline attack, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued a security advisory with mitigation steps to reduce the risk of compromise by ransomware attacks.

The increased involvement of APT groups who engage in cyber warfare would make it extremely difficult to contain ransomware attacks. This was on the agenda for discussion during the recent meeting between President Biden and Russian leader Vladimir Putin. There were similar discussions at the G7 meet in the U.K. in June.

Ransomware needs to be tackled on a global stage, with the involvement of governments, and organizations like Interpol, Europol, NIST, CERT, ACSC (Australia), National Cybersecurity Center (U.K.), and others.

It's about time they banded together and fight back!

INDEX

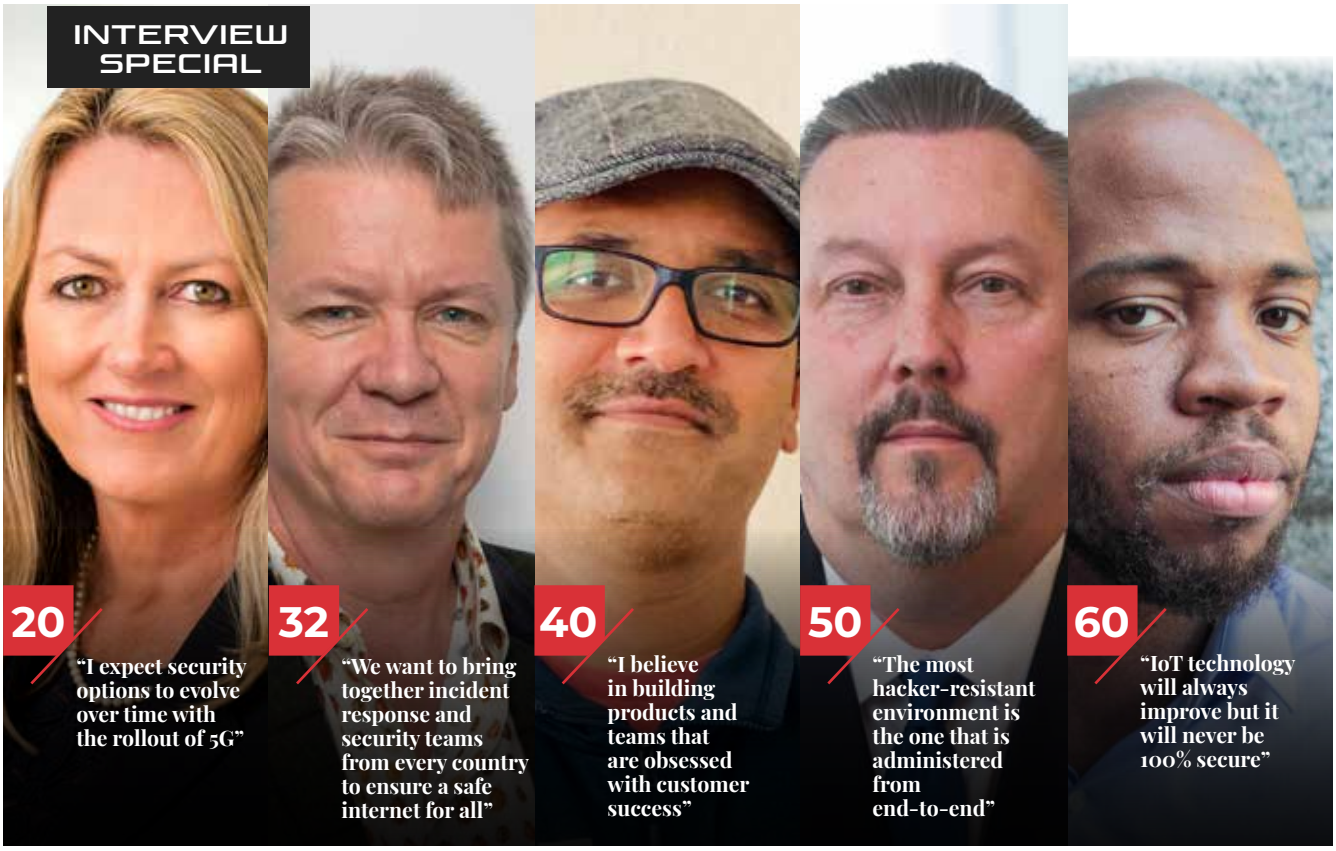
Contents

BUZZ

RANSOMWARE GETS MEATY WITH JBS ATTACK

12

INTERVIEW SPECIAL



20 "I expect security options to evolve over time with the rollout of 5G"

32 "We want to bring together incident response and security teams from every country to ensure a safe internet for all"

40 "I believe in building products and teams that are obsessed with customer success"

50 "The most hacker-resistant environment is the one that is administered from end-to-end"

60 "IoT technology will always improve but it will never be 100% secure"

INSIGHT

The Vulnerabilities that Open the Door to Ransomware

68

KNOWLEDGE HUB

How Communication Service Providers are Keeping the World Connected During COVID-19

78

REWIND

TOP CYBERSECURITY NEWS OF THE MONTH

86

RANSOMWARE GETS MEATY WITH JBS ATTACK

Mihir Bagwe
Sr. Technical Writer
CISO MAG

Ransomware has by far been the buzzword of 2021. Until now, ransomware attacks only appeared under the Tech section of news dailies. However, this has changed. Stories of ransomware attacks are now front page news and make it to cover stories. The modus operandi of ransomware operators has evolved over the years. They are not just looting businesses but targeting critical sectors and larger supply chains, raising the stakes for national security. Remember the Colonial Pipeline hack, which virtually exhausted the entire gas supply on the East Coast? And the Babuk ransomware gang's attack on D.C. Metropolitan Police Department that acted as a roadblock for the law enforcement in the city? These attacks have grown manifold, and are found everywhere.

The dust of the Colonial Pipeline ransomware attack had just begun to settle as the U.S. Department of Justice's (DoJ) newly formed digital extortion task force reported recovering majority of the ransom paid (approximately $2.3 million of $4.4 million in Bitcoins) by the company to the cybercriminals. And while one company was heaving a sigh of relief, another sophisticated ransomware attack took center stage. This time, adversaries struck a meaty blow at the world's largest meat producer – JBS.

SOBRE A
Seara

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost

The Aftermath?

The ransomware attack on JBS' systems did not just affect its IT infrastructure; it had a ripple effect. The attack paralyzed its worldwide supply chain. It halted slaughter operations not just in the U.S. but across its units in Canada and Australia. Transactions and supplies with both – customers and suppliers – were suspended temporarily. The company issued a press release in which it deemed the incident as "organized cybersecurity attack."

Upon discovery, JBS suspended all s
and networks that were known
been intruded on and infor
respective law enforcement au
CISA and FBI.
The only silver-lining in the e

was the fact that JBS had a data backup in place. The company issued a statement confirming that its backup servers were not affected, and thus (they were) actively working with an incident response firm to restore its systems as soon as possible.

JBS did not mention how the ransomware intruded on its systems or the perpetrators involved. But certain news reports suggested that it was the evil hand of the Russian-speaking REvil ransomware gang.
, the notoriously infamous gang
ny details related to the
their underground
"Happy Blog."
tolen

SUBSCRIBE NOW
TO READ THE FULL ISSUE