CISO MAG

beyond cybersecurity

Volume 4 | Issue 02 | February 2020

MANAGED SECURITY

PLUGGING INTO CLOUD

CISO MAG
beyond cybersecurity

Volume 4 | Issue 2
February 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

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

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

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

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

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

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

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

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

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

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

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

Image credits: Shutterstock

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

EDITOR'S NOTE

WHAT IF WE COULD KNOW BEFORE?

Scanning through the headlines on world affairs, I see disturbing news about the Coronavirus (2019-nCoV) in China, which is spreading to other countries. It has now been declared a global health emergency by the World Health Organization. The countries with weaker health systems are likely to be impacted the most. It is also disheartening to read about the number of people who have been infected and quarantined—and the rising death toll. I read a report on the BBC that scientists are already working on the vaccine. Another report says clinical trials could take months and we may not see the tested and approved vaccine until the end of the year. By then, a few more thousands might have died, and the outbreak might end.

Unfortunately, something similar occurs in the cybersecurity world. When a new malware emerges, it can lie hidden in systems for months, gathering information, scanning systems, and profiling users. And then it strikes, leaving little time to react.

But what if we could know all this ahead of time?

What if there was someone continually watching your infrastructure, looking for stealth malware and suspicious activity on your network? They could send you alerts and technical advisories every day or whenever a new malware is discovered in the wild. They could be your eyes and ears so that you could focus on other things that are core to your business.

That's where cybersecurity is heading today.

According to ReportLinker Market Research, the global Managed Security Services market is expected to grow from US$24.05 billion in 2018 to US$47.65 billion by 2023, at a Compound Annual Growth Rate (CAGR) of 14.7 percent during this period.

What is causing demand for Managed Security Services (MSS) and which services are in demand? How do CISOs evaluate security services? What is the technology that is helping to predict a malware attack?

These are some of the questions we address in our cover story, which includes inputs from global CISOs, industry analysts, and Managed Security Service Providers (MSSPs).

The issue you are reading has a new look and a fresh design. Please write to us and let us know what you think about the new design.

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

Jay Bavisi
Editor-in-Chief

INDEX

Diversi

T-Mobile.pl
://azure.microsoft.com
Microsoft Azure
Your vision. Your cloud.
Turn your ideas into solutions faster using a trusted cloud that is designed for you.
Azure. Cloud for all.

SAUDI CYBERSEC SUMMIT 2020

APRIL 21, 2020 | RIYADH

SAFEGUARDING THE KINGDOM'S DIGITAL ECOSYSTEM

events.cisomag.com

#ksacybersec

Block your calendar

APRIL 21, 2020

- Senior Government Leaders
- 25+ Speakers
- 100+ Companies
- 10+ Technology Providers

& More...

CISO MAG beyond cybersecurity

EVENTS

An EC-Council initiative

For more details write to marketing@cisomag.com

HOW SMALL BUSINESSES CAN PROTECT THEMSELVES FROM CYBERATTACKS

Zack Schuler,
Founder & CEO, NINJIO

When most people think of cyberattacks, major data breaches at humongous companies like Equifax and Yahoo, typically come to mind. This is perfectly understandable, as these are the attacks that impact the most people and always make headlines. But cybercriminals don't limit their attacks to large companies—they also target countless small businesses every year. And in many cases, these attacks destroy businesses and livelihoods.

Top 7 Stats from Report

- Every year cyberattacks cost small businesses an average of almost US$80,000, and losses can range up to US$1 million.
- A survey reports 88 percent of small business owners felt their business was vulnerable to a cyberattack.
- Almost two-thirds of small businesses fail to act following a cybersecurity incident.
- 56 percent of SMBs say, defending mobile devices from cyberattacks is extremely challenging.
- The top three attack vectors cited by SMBs are mobile devices, laptops, and cloud systems.
- Just 16 percent of SMBs are "very confident in their cybersecurity readiness."
- 60 percent of SMBs lack a "cyberattack prevention plan."

There's no reason to put it delicately: The state of cybersecurity in the world of small and medium-sized businesses (SMBs) is nothing short of alarming. Not only are SMBs relentlessly targeted by hackers, they're also woefully unprepared to defend themselves and unequipped to handle the aftermath. This is a status quo that has to change immediately—SMBs are the biggest engine of the U.S. economy and they're at risk like never before.

> SMBs are the biggest engine of the U.S. economy and they're at risk like never before.

The Scope of the Problem

Every year, cyberattacks cost small businesses an average of almost US$80,000, and losses can range up to US$1 million (according to a report by the Better Business Bureau). Meanwhile, a 2018 study by the Ponemon Institute found that more than two-thirds of SMBs reported that they had been targeted by a cyberattack within the preceding year. Substantial majorities of SMBs also agree that cyberattacks are becoming more targeted, severe, and sophisticated, but despite these facts, almost half of respondents say they have no understanding of how to protect against cyberattacks.

A recent survey by the U.S. Small Business Administration found that 88 percent of small business owners felt their business was vulnerable to a cyberattack. However, due to resource constraints, a lack of technical expertise, and the rapid pace of change in the cybersecurity world, they often feel helpless or ill-prepared to defend themselves against the vast range of cyberthreats they face.

In fact, a survey of more than 4,100 SMB cybersecurity professionals recently conducted by Forrester, found that almost two-thirds of small businesses fail to act following a cybersecurity incident. Even when the threat is many SMBs don't know