CISO MAG

beyond cybersecurity

Volume 3 | Issue 11 | December 2019

LOOKING BACK ON THE YEAR IN CYBERSECURITY

INDEX

VOLUME 3 ISSUE 11

EDITOR'S NOTE

In the 1985 Robert Zemeckis Sci-Fi movie *Back to the Future*, the film's protagonist Marty McFly, played by Michael J. Fox, gets into his DMC DeLorean/time machine and accidentally goes back in time to 1955. Marty is suddenly in an era that's decades before he was born. He is fascinated to discover the trends and lifestyles of the mid-50s.

Unfortunately, we can't do that!

But we can look back on the trends of the past year and evaluate the predictions made at the beginning of 2019. That's what Chris Roberts, our advisory board member does, in his article titled "Reviewing the Security Predictions for 2019" in the Buzz section.

We get into the DeLorean and set the digital clock to 1976, an era when the Internet was beginning. Michael Moira, SVP & CISO of Korn Ferry writes about his experiences at the beginning of his career helping companies fight early viruses and worms like the Morris Worm and the "I Love You" virus. You can read his story "The History of Security and the Fight to Protect Ourselves" in the Insight section.

For our cover story, titled "2019: A Cyberspace Odyssey," the *CISO MAG* editorial team presents an account of the year at its entirety highlighting the most prominent security incidents of the year. We also name the Cybersecurity Person of the Year.

I end by wishing all our readers a happy and prosperous New Year.

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 11
December 2019

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

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

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

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: Brian Pereira.

VOLUME 3 ISSUE 11

BUZZ

REVIEWING THE SECURITY PREDICTIONS FOR 2019

Chris Roberts, Chief Security Strategist, Attivo Networks

VOLUME 3 ISSUE 11

BUZZ

Around October or November, we throw the collective fortune darts at the nearest board, wall, or screen to work out how the following year's going to be in our electronic world.

We're the digital equivalent of the Farmers' Almanac.

Yet, how often have we really taken a look back and worked out how accurate we've been? How often do we look over our shoulder and assess our success rate and possibly how to improve our accuracy?

So, this year, instead of grabbing the nearest intern, developer, or passing user and practicing the art of extispicy like haruspices on them to work out what we're going to be looking at in 2020, we're going to take a look back at some of the 2019 predictions and have a little dig around the Internet to see how well the prognosticators faired.

If one of these predictions is yours or you were the one who copied it, rebranded it, and made it your company's, then accept the criticism and be a little more careful with how you read this coming year's entrails, as there are now consequences. You will be held responsible!

So, without further ado, let's start with some of the cringe worthy ones:

Rates of ransomware attacks will fall (Kiuwan)

I'm going to say this hasn't been the case, and even if it can be found that the actual number of attacks in a country has decreased, then the effects and overall challenges with the attacks has significantly increased, especially in the case of many local, state, and government agencies, let alone the school districts and healthcare facilities. If you look at the statistics being quoted around the "every 14 seconds a business falls victim to a ransomware attack" we're NOW down to 11 seconds, so this one's been solidly sunk and we still have to deal with ransomware and all $11 billion worth of damages.

AI will be a major force in information security (multiple sources for both defense and attack)

Ok, this one's partly true, but unfortunately not in the way we really want to see it. Marketing, sales, and all companies that blink in the night have taken up the cry of "AI will save us!". As far as the eye can see, it's a forest of AI marketing, explaining how their solution's going to solve your problems and cook you breakfast in the morning, and most of it is utter codswallop. At best they've created an augmented system of pattern matching rules and assume the recommendations can now be called AI. We won't even talk about their training models, their update capabilities, or understanding of how to scale and justify an ROI based on cost savings or increased maturity on the security scale. Please do right by all of us, stop throwing good money after bad and really dig into any AI solution to see what actually makes it tick and remember: all that glitters is not gold.

VOLUME 3 ISSUE 11

BUZZ

IoT regulations will finally be addressed (Alvarez)

We'll go with partial credit on this one. Firstly, yes, the regulations are coming and it's got NIST (National Institute of Standards and Technology) at the helm. The problem is, various NIST regulations appear to be held up and have been eaten by the "swamp" or various parties within it. The IoT Cybersecurity Improvement Act (1668) is languishing somewhere in DC, and the Office of Management and Budgets or the Office of Information and Regulatory Affairs has eaten 800-53, which as we all know is one of the backbones of our industry. So, if someone in charge in DC is reading this, can you please finally finish red-lining all the stuff we need? Believe me, you, your friends, families, companies and the entire information security ecosystem will be better off for these things actually getting out of your hands and back to NIST's and then out to the general population. Until that time, IoT's a mess, in all likelihood your toaster probably hacked the fridge, which is connected to the Internet and is therefore mining cryptocurrency. What a mess.

GDPR will have a significant impact (multiple sources)

If you define a significant impact as making us more aware as to how badly we're doing in information security then yep, we've doubled (or more) the number of breaches being reported. But, the regulation has been absolutely ineffective at levying sanctions, fines, or other legal actions against the companies that still fail to adequately protect our very data. The upside is that a unified front on notification is a good thing; the downside is the sheer volume of notifications simply shows us that we're not having an impact on stemming the flow of data being stolen, let alone holding the industry or the enterprises accountable for the losses. It will be interesting to see if the U.S. takes note and learns from the colonial cousins across the pond or simply continues to tackle the problem in the patchwork fashion of 50 small independent countries (mostly) united under one flag.

HONORABLE MENTIONS:

Defenders will think and operate like the attackers (Our own company) and companies will focus on their cyber hygiene of their own environments (Illusive Networks)

So, taking both Attivo and one of our competitors to task for these ones. It is something we want, something we aim for, and something we would like to see in the industry. More focus on defense, more focus on giving the blue teams some teeth, more time, effort, and budget spent developing the defensive, detection, deception, and proactive arms of the organizations out there…but, reality is very different. Many companies are struggling to understand what they have, where it is, and what to do with it, all with limited resources and a plethora of regulatory and compliance directives to adhere to. It's a real problem, and one that needs focus. The time has to be spent on helping to educate organizations, to work with them, develop roadmaps, run training, tabletops, and effectively act as their advocate in the industry. If we can take the time to do this, and we can bring our own industry into line, then, and only then I think we can make a difference and then the defenders will have the time to "think like the attacker" as opposed to firefighting on a daily basis.