WISHING YOU A

HAPPY

New Year

TEAM CISO MAG
EDITOR'S NOTE

CYBERATTACKS WILL MOVE TO A HIGHER LEVEL

I begin this note by wishing all our readers, patrons, contributors, business partners, and fans a Very Happy and Healthy New Year!

Yes, health and health care are going to be important considerations for the world in 2021. I am optimistic that, with the availability of vaccines, the world will limp back to normalcy this year. With that, the rate of unemployment should drop, and the crime graph will also dip. And hopefully, cybercriminals will mend their ways.

Yet, it is worrisome to see cybercriminals moving to sophisticated agendas, like their involvement in cyber warfare and attacks on critical infrastructure, with malicious intentions of disrupting life and destabilizing economies. Attacking nuclear facilities (Iran) or turning off the national grid used to be the stuff of James Bond and Mission Impossible movies. It's very much a reality today. And it makes those sell credit card numbers on the dark web look like rookies.

Thirty years ago, hackers were contented with attacking browsers or applications and disrupting enterprise networks. They pursued intellectual property and customer data – and sold that to competitors. But today, they are after something much bigger than that.

For our first issue of 2021, we spoke to many industry professionals to validate our beliefs about what we think could be the leading cybersecurity trends. Read what the cybersecurity pundits predict in our INSIGHT section on page 20.

Don't miss our Cover Story, 5 Cybersecurity Approaches That All Businesses Should Consider in 2021, on page 50. It offers wisdom and advice for CISOs.

I can confidently say that the trends will align to the pandemic - as work from home continues, and supply chains are reconfigured. Bad actors will choose to exploit the naivety of gullible folks, this time turning their attention to vaccine distribution and health insurance fraud. And since we shop online more often, they will target e-commerce sites and logistics companies too.

So, please be prudent and mindful about emails or tests from people impersonating health authorities or from fake insurance or logistics companies.

The bad guys are also going to up their game and look at new modes of attack – like deepfakes – and the use of artificial intelligence. Don't be surprised to see more deepfake news videos that sound and look so much like the real thing. And if you get a call from your CEO or CFO, which sounds so much like them, would you fall for it? It could be a case of deepfake – yes, the bad guys can do voices too, like the late Hollywood actor Robin Williams (watch the 1993 American comedy-film Mrs. Doubtfire). That's taking spear-phishing and whaling to a whole new level!

So, adopt a zero-trust policy, even at a personal level. And do verify by making a few calls.

Stay safe, cautious, and healthy in 2021.

Please write to us at cisomag@ecouncil.org.
Cybersecurity In Industry experts reflect on what happened in 2020 and make predictions about what to expect in 2021

20

Contents

Cybersecurity In Industry experts reflect on what happened in 2020 and make predictions about what to expect in 2021

08

Buzz

Under the Spotlight

“Invalidation of the EU-U.S. Privacy Shield was a long time coming”

Robert Meyers
Channel Solutions Architect, One Identity

14

Insight

Cybersecurity In

20

Cover Story

5 Cybersecurity Approaches All Businesses Should Consider in 2021

42

Vendor Relationships: Soft Skills for CISOs

50

Knowledge Hub

“Ivalidation of the EU-U.S. Privacy Shield was a long time coming”

Robert Meyers
Channel Solutions Architect, One Identity

14

Insight

Cybersecurity In Industry experts reflect on what happened in 2020 and make predictions about what to expect in 2021

20

Table Talk

“Owing to a lack of security awareness, the abuse of DNS server vulnerabilities is still not taken very seriously”

Donny Chong
Product Director, Nexusguard

56

Industries

“Owing to a lack of security awareness, the abuse of DNS server vulnerabilities is still not taken very seriously”

Donny Chong
Product Director, Nexusguard

56

Industries

“The battle for the vaccine market to launch cyberattacks has already begun”

Dmitry Volkov
Co-founder, Group-IB

62

Industries

“The battle for the vaccine market to launch cyberattacks has already begun”

Dmitry Volkov
Co-founder, Group-IB

62

Industries

“Owing to a lack of security awareness, the abuse of DNS server vulnerabilities is still not taken very seriously”

Donny Chong
Product Director, Nexusguard

56

Industries

“The battle for the vaccine market to launch cyberattacks has already begun”

Dmitry Volkov
Co-founder, Group-IB

62

Industries

“Owing to a lack of security awareness, the abuse of DNS server vulnerabilities is still not taken very seriously”

Donny Chong
Product Director, Nexusguard

56

Industries
CYBERSECURITY
What to Expect in 2021

Safi Raza
Director of Cybersecurity
Fusion Risk Management
The year 2020 witnessed a seismic physical, economic, and cultural shift among global organizations, as businesses adapted to working during a pandemic.

When COVID-19 brought sweeping changes to the way we operate, communicate, and do business, cybercriminals were in the wings waiting to seize the opportunity to exploit security weaknesses for monetary and disruptive gains. In light of this, we’ve experienced a sharp rise in cyberattacks across a range of industries including health care, education, and e-commerce. Today, cybercriminals are constantly evolving to take advantage of online behavior and trends and the COVID-19 pandemic is no exception to this.

So, what will cybercriminals bring to the table in 2021? How do organizations ensure they have the appropriate cybersecurity strategy in place to mitigate the ever-changing and evolving cyber threats?

The Rising Risk of Remote Working

Today, most organizations have a remote workforce, and many employees are relying on personal devices to conduct work – this method of working is not secure. Why? Remote employees are sharing the home network with smart TVs, phones, tablets, and various IoT devices that are not adequately secured. The exchange of highly sensitive and confidential information that once occurred behind the fortified infrastructures is now being conducted from fragile home networks.

For the modern CTO, this situation is not ideal. As home working cyber-related risks will only become greater during the next year, CTOs and their teams are relentlessly exploring avenues to help mitigate cyber risk. In 2021, organizations will need to spend more time and money on endpoint security and end-user training.

AI: The Future of Cybersecurity

The massive and sudden increase in the number of people working from home has furthermore validated the role of artificial intelligence (AI) in the future of cybersecurity. Unlike traditional security solutions, AI does not depend on known signatures. Instead, it relies on user and attack behavior analytics and network traffic analytics, quickly neutralizing a threat before it becomes a crisis.

Phishing is the most commonly known threat countered by the use of AI. Microsoft and Google already use AI to detect spam and phishing emails. Several cybersecurity companies including Rapid7, Dark Trace, Barracuda, and Palo Alto are using AI-powered SIEM, firewalls, and a variety of other applications to ensure organizations remain secure.

The implementation of AI and Machine Learning helps us identify attacks by being able to analyze and predict attacks in real-time. In 2021, we will see much more of this as organizations invest in avoiding cyberattacks before they become a threat.

Social Engineering - The Dangers of Deep Fakes

Employees are the weakest link in the defense of data.

Ransomware: A Threat

Cybercriminals follow the money. In ransomware cases it will continue to resonate. They use a tool for as long as it is effective against victims of ransomware.

Infrastructure Security

Department of Homeland Security warned that...