CISO MAG

beyond cybersecurity

Volume 2 | Issue 1 | February 2018

CYBERSECURITY THE PHOENIX SAGA

Evolved over billions of years...

Protecting your enterprise in one hour.

The immune system has evolved over billions of years. But it takes just one hour to install one in your enterprise.

Using machine learning, Darktrace can tell friend from foe, and catches threats that others miss. Even if they've never been seen before.

From quiet insider threats and zero-day attacks, to hacks of connected devices or industrial networks, our software sees it and responds.

Find out what's lurking inside your systems.

darktrace.com

"Darktrace AI detects threats that others miss."

William Reid, Wyndham New Yorker

DARKTRACE
World-Leading Cyber AI

INDEX

EDITOR'S NOTE

The year of 2017 witnessed some of the most brutal cybersecurity meltdowns. The breaches were not always directed toward corporates; some were state-sponsored which did colossal damage to an inordinate number of Internet users. While Equifax and Yahoo stole the headlines with massive breaches, a number of cybersecurity facepalms—like Uber and Deloitte—didn't go unnoticed.

The year 2017 may have created mayhem for information security professionals, but it left them better prepared as well. Some organizations adopted a coordinated approach to cyber risk management and several nations spruced up their cyber divisions in the aftermath of the attacks. Our cover story "Cybersecurity: The Phoenix Saga" takes a look back at the brighter moments of 2017 and suggests that all is not lost.

Move to our Buzz section, where we discuss how cybercrime has jolted the pharma industry and become its biggest health hazard. The feature also suggests selective measures pharma companies can employ to safeguard themselves against intellectual property theft.

In our Under the Spotlight section, we have JA Chowdary, Special Chief Secretary & IT Advisor to Chief Minister of the Indian state of Andhra Pradesh. He discusses his vision for Fintech Valley in Vizag, Andhra Pradesh, and his efforts for continued development of the Fintech ecosystem in India.

We also interviewed Kelly Isikoff of RenaissanceRe, where she discusses cybersecurity practices in the insurance sector, women representation in the cyber world, and much more.

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 2 | Issue 1
February 2018

Editorial
International Editor
Amber Pedroncelli
amber.pedroncelli@eccouncil.org

Senior Editor
Rahul Arora
rahul.arora@eccouncil.org

Feature Writer
Nishtha Pathak
nishtha.p@eccouncil.org

Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Media and Design
Media Director
Saba Mohammad
saba.mohammad@eccouncil.org

Design Head and Visualizer
MSH Rabbani
rabbani@eccouncil.org

Designer
Jeevana Rao Jinaga
jeevana.j@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

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

Marketing & Sales
General Manager
Meghana Vyas
meghana.vyas@eccouncil.org

Marketing Manager
Pooja Saga
pooja.saga@eccouncil.org

Sales Manager - India
Basant Das
basant.das@eccouncil.org

Sales Manager - North America
Jessica Johnson
jessica.johnson@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: Rahul Arora.

CYBERCRIME: A SERIOUS HEALTH HAZARD

Augustin Kurian

The pharma industry has always been in a tight spot. Keeping up with medical advancements and staying revolutionary in the space are just a couple of the many challenges they face. There is only one constant: the challenges and threats the industry has faced for decades. With technological innovations, cybercrime has joined this new legion of threats to the healthcare technology industry. In fact, a 2015 survey by Crown Records Management revealed that two-thirds of pharma firms had faced data breaches—with one-fourth of these firms reporting they wavictims of cyber attacks. In late October 2016, Northern Lincolnshire and Goole NHS Foundation Trust in the United Kingdom was targeted by a malware attack. Several operations scheduled on that day had to be cancelled, with some trauma patients forced to redirect to a different location. The United States fared no better, reporting an 18.5 percent increase in the pharma sector in 2016 compared to the previous year.

This culminated in May 2017 after the WannaCry attack crippled the UK's National Health Service along with several other companies and establishments. Hospitals and GP surgeries in England and Scotland were among the worst hit. Hospital staff were forced to resort to pen and paper, and their own cell phones because the attack affected key systems, including telephones. Operations, surgeries, and several appointments had to be cancelled after the malware scrambled data networks. The only wing functioning at affected hospitals was emergency medical care. The crypto-worm targeted Windows computers using the EternalBlue exploit, taking advantage of Windows' Server Message Block (SMB) protocol and installing a backdoor implant tool called Double Pulsar. Then, the crypto-worm transferred and ran the WannaCry ransomware package, which, in turn, encrypted data and demanded a ransom from victims in the form of Bitcoin. The attack is among the most infamous ransomware attacks ever, affecting more than 150 countries and 230,000 computers.

The WannaCry attack was a reality check to several pharmaceutical organizations. Following the incident, the industry saw cyber-attacks as a harbinger of several other major attacks the industry was poised to face. This was followed by the ECRI Institute announcing the "Top 10 Health Technology Hazards for 2018 list," which ranked cybersecurity as the number one threat to healthcare technology.

"This year's No. 1 hazard calls attention to the patient safety component of ransomware and other cybersecurity threats. In the healthcare environment, ransomware and other types of malware attacks are more than just an IT nightmare. They are potential patient safety crises that can disrupt healthcare delivery operations, placing patients at risk. Multiple ransomware and other malware variants have infected healthcare organizations, as well as other private and public organizations, throughout the world," ECRI stated. "Patient safety is on everyone's mind, but technology safety sometimes gets left behind," added David T. Jamison, Executive Director of the Health Devices Group, ECRI Institute.

WHY THE PHARMA INDUSTRY?

Simply put, healthcare records are valuable on the Dark Web, which is where black market drug sales occur most often. Pharmaceutical firms create and manage a large amount of intellectual property and data, which can include patient profiles and drugs that are currently in the development cycle (or are already developed). The research and development of these drugs is already cost-intensive for these companies, which makes holding them for ransom so easy to do.

Pharma firms are also targeted due to geopolitical reasons. Most of these companies are based outside of the U.S., making them a favorite of state-sponsored actors and extremist groups. According to a study by Deloitte titled "Cyber & Insider Risk at a Glance: The Pharmaceutical Industry":

"Evidence abounds that pharmaceutical companies are the target of sophisticated Internet criminals. The UK Government identified pharmaceutical companies as the primary target of cyber criminals bent on stealing IP. It estimated cyber-theft of IP cost the UK £9.2b, of which it attributed £1.8b to theft of pharmaceutical, biotechnology, and healthcare IP. Surveys of U.S. cyber attacks consistently find that pharmaceutical IP is a major target of sophisticated cyber gangs. Experts suggest China is using cyber-espionage to support its 5- year economic development plan.

That plan includes expanding China's chemical and pharmaceutical sector. Attacks against major U.S. pharmaceutical companies attributed to sophisticated Chinese hacking groups include Boston Scientific (a medical device-maker), Abbott Laboratories, and Wyeth, the drug maker acquired by Pfizer Inc. The same group successfully hacked the Food & Drug Administration's computer center in Maryland, exposing sensitive data (including formulas and trial data) for virtually all drugs sold in the U.S."

Sometimes, even hacktivists come into the picture, as many of the drugs are quite expensive. Hackers attempt to access proprietary information and disclose data that the firms usually keep confidential.

REGULATORY GLITCHES IN PHARMA CYBERSECURITY

Anne Petterd, Principal of Baker McKenzie Wong & Leow, in an interview with Health Care Innovation explained: "In terms of data sovereignty—where a jurisdiction places restrictions on taking data beyond its borders—healthcare data is an issue which comes up frequently when parties are trying to negotiate free trade agreements. There's a notion that if the data is within the country, it may be more accessible to those who need it, be it the patients or the healthcare providers. There's also the notion among regulators that if the data is within the country, it may be more secure. However, if you speak to the cloud providers, particularly those who spend a lot of time investing in security for their products, this may be one of the main issues that they want to discuss with regulators as to whether that is really true. Companies may want to deliver services from one central location for efficiencies across borders, and with that comes savings in terms of time and storage of data, especially when it comes to big data analytics. This is an issue that healthcare companies may feel is constraining them with what they want to do in the region."

She continued by saying: "It's a constant balancing that regulators need to do. Even if a law has been passed that strikes the perfect balance, something might change the next day which means the system is no longer in balance."

She also highlighted that following the WannaCry incident, "The UK government conducted several audits and reviews. One of the recommendations on striking the right balance suggests giving patients more control and choice over who their electronic records can be shared with."

WHAT CAN BE DONE?

The pharma industry has possibly the world's largest research and development sector. It is the duty of the CISOs/CIOs to make sure that customer data, intellectual property, and every other valuable asset are protected; more importantly, the companies must have a cybersecurity department at its disposal. Cybersecurity must originate from the foundation of the company—and it must be performed in tandem with the lifecycle of the firm.

It must never be an afterthought.

The attackers are evolving and keeping pace with them is of paramount importance. According to New Hampshire-based Elliot Health System's Chief Information Security Officer Andrew Seward, "You can set the conditions for success." Seward offered this advice in an interview with Healthcare IT News. "You can't know everything, but you can never go wrong with hiring the right people and building a condition of trust."

He continued, "It takes forward-thinking individuals who can see the risk and determine security is a business risk. When you're doing futureproofing, you have to determine how much is enough to manage security, and then how much security is enough."