



**CISO
MAG**

beyond cybersecurity

Volume 2 | Issue 7 | August 2018

APT

**FINDING A NEEDLE IN A
MILLION BARNS**

CYBERSEC SERIES

CONTACT US

Alliances & Delegate Registrations

Rakesh Acharya
rakesh.acharya@eccouncil.org
+91-79778-28905

Sponsorship Opportunities

Renaldo Howell
renaldo.h@eccouncil.org
+91-79955-64887

Speaking Opportunities

Jyoti Punjabi
jyoti.punjabi@eccouncil.org
+91- 99636-54422

 **OMAN**
CyberSec Summit

30th October 2018 | Muscat

 **SAUDI**
CyberSec Summit

13th November 2018 | Riyadh

 **QATAR**
CyberSec Summit

28th November 2018 | Doha

Strategic Partners



**BATTERJEE EDUCATION
AND TRAINING ACADEMY**

Exclusive Media Partner





10

BUZZ

Boards Should Tighten Cybersecurity Oversight



18

COVER STORY

APT: Finding a Needle in a Million Bams



28

UNDER THE SPOTLIGHT

Kevin Stallard
Senior Enterprise Security Architect, US Bank



42

COLLABORATIONS

Infosec Partnerships



50

IN THE NEWS

Top Stories from the Cybersecurity World



56

IN THE HOTSEAT

High-Profile Appointments in the Cybersecurity World



62

KICKSTARTERS

Startups Making Waves in the Cybersecurity World



EDITOR'S NOTE

It takes well over a month for enterprises to patch a critical vulnerability, let alone prevent an attack. With the threat landscape evolving at a rapid pace and advanced

attacks from state-sponsored actors continuing to be the most difficult ones to be identified, it is imperative that companies are equipped with technological infrastructures that help them quickly identify and remediate advanced persistent threats (APT). In our Cover Story, we discuss how advanced threats have wreaked havoc for decades, with the case studies of Stuxnet, the world's first digital weapon, and the great bank robbery of the Carbanak APT.

Move to our Buzz section where Dottie Schindlinger, Vice President & Governance Technology Evangelist for the Diligent Corporation, talks about how boards should tighten cybersecurity oversight—starting with themselves. She also discusses the role of CISOs in educating the board about cyber risk and shaping the board's crisis response plan.

In our Under the Spotlight section, we interview Kevin Stallard, Senior Enterprise Security Architect, US Bank, on application security, how much coding a CISO should know, what makes a good engineer, and 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



Volume 2 | Issue 7
August 2018

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

Senior Editor
Rahul Arora
rahul.arora@eccouncil.org

Senior Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Media and Design
Media Director
Saba Mohammad
saba.mohammad@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 and Business Development
Officer
Pooja Saga
pooja.saga@eccouncil.org

Riddhi Chandra
riddhi.c@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. 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.

AI-Driven Managed Detection and Response



- Detect Threats 85% Faster
- Eliminate False Positives
- Get Swift Incident Analysis
- Respond in Near Real-time



“Paladion Combines MSS and MDR for a Holistic Approach to [Cyber] Security Services” **451 Research**

Partner with Paladion's AI-Driven Managed Detection and Response to stop attackers before there is a catastrophic breach.
Visit www.paladion.net or call +91-9741115000

The Ivanti logo, consisting of the word "ivanti" in white lowercase letters on a red rectangular background.

ivanti

PROTECT PERSONAL DATA

Mitigate up to
95%

of today's Cyber Attacks.
Proven security from Ivanti

Boards Should Tighten Cybersecurity Oversight—Starting with Themselves

Dottie Schindlinger
Vice President & Governance Technology Evangelist
Diligent Corporation

In the wake of the many high-profile data breaches in the news recently, many boards are striving to step up their cybersecurity oversight. However, progress has been slow. A January 2018 [survey](#) by Marsh and Microsoft found that 70 percent of board members ranked cyber risk as a top concern, but only 14 percent were “highly confident” in their company’s ability to respond to a cyber-attack.

Why this mismatch? Unfortunately, responsibility may partly rest with boards themselves. Improving cybersecurity requires a major culture shift—everyone at an organization needs to change their behavior to mitigate risk, from the board and executive team on down. However, too many boards are themselves not following best practices for cyber preparedness, setting a less than stellar example for those lower in the hierarchy.

For example, a 2017 [survey](#) conducted by Diligent and NYSE Governance Services found that 92 percent of board directors report using personal email – at least occasionally – for board communications. That’s a risky practice that could open the organization to [embarrassing leaks of private information](#), or in the worst case, revelations of corporate secrets.

Luckily, CISOs can share and advocate for a few simple strategies that can greatly mitigate board directors’ risk of being hacked—and support a strong cybersecurity culture throughout their organization.

Take the Lead on Educating the Board About Cyber Risks

One of the main challenges that CISOs face is educating the board about the intricacies of cyber risk. Even for the most engaged board members, cybersecurity is an incredibly complex and intricate area of oversight. It is also a relatively new area of oversight, so most board members will not have had experience with it throughout the course of their careers.

“Traditional operating and compliance risks are well described. There is historic benchmark data to learn from,” said Dr. Anastassia Lauterbach, an entrepreneur and investor who serves on the board of commercial data and analytics company Dun & Bradstreet. “Cyber risk, however, can’t be boxed into one corporate function, limited to one particular geography, or handled by a consultancy.”

It is feasible that board members may be unaware of the myriad of cyber risks that companies face, including leaks from inside, DDoS attacks, and unsecured IoT devices. According to a 2017 ISACA [report](#), only 21 percent of board directors are briefed on cybersecurity and other risk topics at every leadership meeting. Helping boards understand the full scope of the problem—and their organizations’ unique vulnerabilities—is a key job for CISOs.

With this in mind, CISOs should advocate to present directly to the board in person at regular intervals throughout the year. Providing expert cybersecurity insight at this top level can help

boards understand the full scope of cyber risk, and will give them an opportunity to raise questions and plug gaps in their knowledge. It can also help ensure that discussions about cyber risk are regularly on the board meeting agenda, in line with [recommendations](#) from the National Association of Corporate Directors (NACD).

An equally important task for CISOs is to advocate cybersecurity training for all board members. This will help ensure that there are experienced individuals who can identify the connections between cybersecurity and overall company strategy sitting in those boardroom seats.

That same Diligent and NYSE survey found that 62 percent of board directors are not required by their organizations to undergo cybersecurity training—a major oversight. In an age when cybercrime costs the average company \$11.7 million a year, according to [Accenture](#), leaving oversight to the IT department is no longer an option for companies.

Thoroughly Vet Apps and Software Used by the Board to Communicate

Most business departments are supported by dozens of software programs and online services that help employees do their jobs more efficiently and quickly. By contrast, most boards continue to rely on conference lines and PDFs shared by email—systems that have barely changed since the 1990s. Even the most unsophisticated hacker can access confidential and classified information on an [unencrypted on a USB stick](#).

But in order to make well-reasoned decisions about cybersecurity policies, boards need to be familiar with the modern apps, platforms, and devices those policies are meant to protect. While CISOs have little control over what technology directors use on their own time, they can encourage boards to adopt up-to-date enterprise governance management software. Switching to paperless document sharing or secure messaging platforms can nudge board directors toward familiarizing themselves with new technologies—and the many different layers of security they require.

Shape the Board's Crisis Response Plan

According to Accenture, a company has an average 130 cybersecurity breaches each year. For most large organizations, it's only a matter of time before one of those breaches are big enough to make headlines.

Therefore, CISOs must ensure that there is an open, continuous, and honest line of communication between IT staff and the board; one study found that 60 percent of IT staff do not report cybersecurity risks until they are urgent, and, therefore, more difficult to mitigate. Many also acknowledged that they try to filter negative results.

An insufficiently timely and sensitive response to such a crisis can do serious damage to a company's reputation and bottom line. For instance, the public outcry against Facebook in the wake of [the Cambridge Analytica scandal](#) was worsened by [reports](#) that Facebook had known about

the data breach for more than two years, but had never alerted any of the 50 million users who were affected. In the week after the story broke, Facebook's stock plummeted, shaving [\\$100 billion](#) off the tech giant's market cap.

Creating a comprehensive crisis response plan can help avoid that kind of blowback; if and when a cybersecurity scandal breaks, board members should know exactly what will happen and what their [response](#) will be. However, the Marsh and Microsoft survey found that only 30 percent of organizations currently have such a plan in place—and those that do, have not reviewed or updated their plans since they were initially developed, according to NADC. CISOs must help keep boards informed about current cybersecurity regulation to ensure that their actions are in-line with current legal requirements.

These days, it's a question of when an organization will be hacked rather than if. By helping to create an educated and aware board, CISOs will be instrumental in supporting a cultural shift toward more secure cyber practices in their organizations—and ensure that the impact of such an attack, when it comes, will be limited. 🔒

Dottie Schindlinger is Vice President & Governance Technology Evangelist for the Diligent Corporation, where she promotes the intersection of board governance and technology as a recognized expert in the field. Dottie writes and presents on governance and technology related topics and the Diligent Governance Cloud through a variety of digital and print publications, webinars, conferences, and boardroom presentations to directors and executives globally.

The opinions expressed within this article are the personal opinions of the author. The facts and opinions appearing in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.



TAKE YOUR HACKING BY STORM

The Storm Mobile Security Toolkit is mobile training on a versatile, portable Raspberry Pi-based, touchscreen, tailor-made system. It is a customized, customizable*, fully-loaded pen test platform!

The Storm comes equipped with a customized distro of Kali Linux and the course of your choice (or 2) on the device.

RETAIL \$749 | DISCOUNT \$699

Use code **CISOMAG** at checkout to get your discount.

TOOL KIT CONTENTS

- ✓ 64Bit - Quad Core Mobile System
- ✓ 1GB RAM
- ✓ 7" touch screen display
- ✓ 64GB MicroSD - Preloaded w/Custom Linux Hacking OS
- ✓ 100Mb Ethernet port
- ✓ 4 USB ports
- ✓ 802.11n wireless
- ✓ Bluetooth 4.1
- ✓ Combined 3.5mm audio jack and composite video
- ✓ Camera interface (CSI)
- ✓ Display interface (DSI)
- ✓ VideoCore IV 3D graphics core
- ✓ Full HDMI
- ✓ USB Micro Power Cable
- ✓ Rollup water resistant keyboard
- ✓ Field Case Organizer for all your gear

WIRELESS HACKING
WIRED HACKING
RF HACKING

* Customize at your own risk. You assume the responsibility for your device. No warranty is implied or given.

18
ATT

FINDING A NEEDLE IN A MILLION BARNES

19
Augustin Kurian

In 2010, a team of inspectors from International Atomic Energy Agency at Natanz, Iran, noticed that the centrifuges at a uranium enrichment plant were consistently and mysteriously failing. Five months later, some computers began crashing and rebooting repeatedly. The team trying to troubleshoot the issue did the routine checks, anticipating the problem would be malware. But it wasn't like any other worm or virus they had come across. The malware went on to wreak havoc in the nuclear facility. What they didn't know was that they had stumbled upon the world's first digital weapon: Stuxnet.

Stuxnet, the 500kb worm, infected 14 uranium-enrichment plants in Iran. The malware relied on unsuspecting victims installing it and then spreading it over the network. It first targeted Microsoft Windows computers, proliferating into the system, and the network. Then, it targeted Siemens Step7 software, which was used to operate the centrifuges. Stuxnet compromised the centrifuges, spinning them out of control in order to tear them apart. It became clear that Stuxnet was the new face of 21st-century warfare: invisible, anonymous, and devastating.

Post Stuxnet, Iran retaliated with cyber espionage on Israel and its allies. In 2012, Saudi Aramco was attacked. More than three-fourths of their main computer network was destroyed and over 30,000 hard drives of Aramco personal computers were wiped. The hackers identified themselves as Cutting Sword of Justice. Saudi accused Iran of the attacks. This triggered escalating cyberwarfare; Iran was attacked by advanced

malware campaigns like the Dugu and Flame attack, targeting the oil and gas operations of the country. Iran responded by releasing the next-gen Shamoon on Saudi banks. In 2013, Iran hacked New York dam, and several American banks including JP Morgan Chase & Co., Bank of America Corp., Wells Fargo & Co. and PNC Financial Services Group Inc., and later, Las Vegas Sands.

Stuxnet was considered one of the very first examples of an effective deployment of an Advanced Persistent Threat or APT (a term originally coined in 2006 by Colonel Greg Rattray of the United States Air Force while discussing data-exfiltration Trojan attacks), which triggered global cyber warfare.

Though APTs only account for about 20 percent of all cyber-attacks, if successful in its execution, the severity of APTs is massive and, at times, irreparable. Among the few recent and noteworthy executions of APT was [The Great Bank Robbery: the Carbanak APT](#), one of the most successful APT campaigns ever created which defrauded nearly \$1 billion from European and the United States banks.

"The story of Carbanak began when a bank from Ukraine asked us to help with a forensic investigation. Money was being mysteriously stolen from ATMs. Our initial thoughts tended towards the Tyupkin malware. However, upon investigating the hard disk of the ATM system we couldn't find anything except a rather odd VPN configuration (the netmask was set to 172.0.0.0)," stated the researchers from Kaspersky Labs in the blog [Secure List](#).

The story of Carbanak began when a bank from Ukraine asked us to help with a forensic investigation. Money was being mysteriously stolen from ATMs. Our initial thoughts tended towards the Tyupkin malware. However, upon investigating the hard disk of the ATM system, we couldn't find anything except a rather odd VPN configuration (the netmask was set to 172.0.0.0)



It continued. "At this time, we reported a major cyber incident attack, but we knew that for a few months later one of our colleagues would receive a call at 1 a.m. in the middle of the night for the phone was an unusual message, asking for a certain number a matter of urgency. The person at the end of the line was the CEO of a Russian bank. One of their operations was starting that day and they were from the Russian Consulate in the People's Republic of China," according to the team of Espionage research conducted upon the APT. "When we arrived in the morning, quickly after it had the malware on the system. We made a back-escape that removed the malware from an infected PC and ran the script on all the computers in the bank. The next day, multiple times, we saw that all the machines were clean. 12 hours, maybe more, and then, through them, we determined the Cyberbank malware for the first time."

Cyberbank used a string of malware structures upon phishing and used a compromising financial transaction from APTs, money transfer, and even small profit of the system. The malware, which was designed for espionage and data collection, was sent as an attachment in the e-mail. Once installed as a system, the malware enabled structure to move through the network to identify and collect computers that could be used for financial transactions on APTs and other systems. These infected computers were used to collect various of data and collect other types of intelligence that were

then sent back to the control system. "Even though the quality of the virus was relatively good, they were still good enough for the structure, which also with the two infected files for the phishing machine is understood what the virus was doing. The provided files with the knowledge that needed to call out the system, according to [redacted] info."

Despite under the APTs, the infected files of infected files from banks and various other critical infrastructure. These files include the list of companies in the stock and internet system as well as the list of public institutions and the government's agencies.

"Today, most of the organizations in a bank the infected part of the network are protected by multiple layers of security, determining from firewall, DMZ, antivirus, anti-spam programs, etc. The attack has no longer been using a single malware with multiple APTs infrastructure, although it has become a more complex with the use of an infected to identify patterns. Since APT, which is one of the advanced in the world, we can expect the future will be further for structure," said the first operator and lead, Phishing Training, CMC, expert, Rafael Almeida.

He continues, "APT, which is the most dangerous, persistent and persistent. The attack single comes a chain of activities for the infected system. Some have followed in the attack on the infrastructure for phishing, espionage and data collection."

SUBSCRIBE NOW
FOR COMPLETE ISSUE