UNMASKED

CYBRARY.IT

TAKING THE MYSTERY OUT OF CYBER SECURITY

MARCH 2018 | EDITION 1

IN THIS ISSUE

EDITOR'S NOTE

You may have noticed a recent change to the Cybrary homepage. We want users to be able to track the daily trending topics and have a sense of where their assessment scores lie on the leaderboard.

Engagement with content in any form is a great way to learn, even if it's spending 5 minutes browsing the 'What's Hot' section each day.

You may have also noticed some new colors and imagery being used across the site. More details about the Cybrary rebranding are coming soon! In the meantime, check out the **Cybrary homepage** if you haven't already.

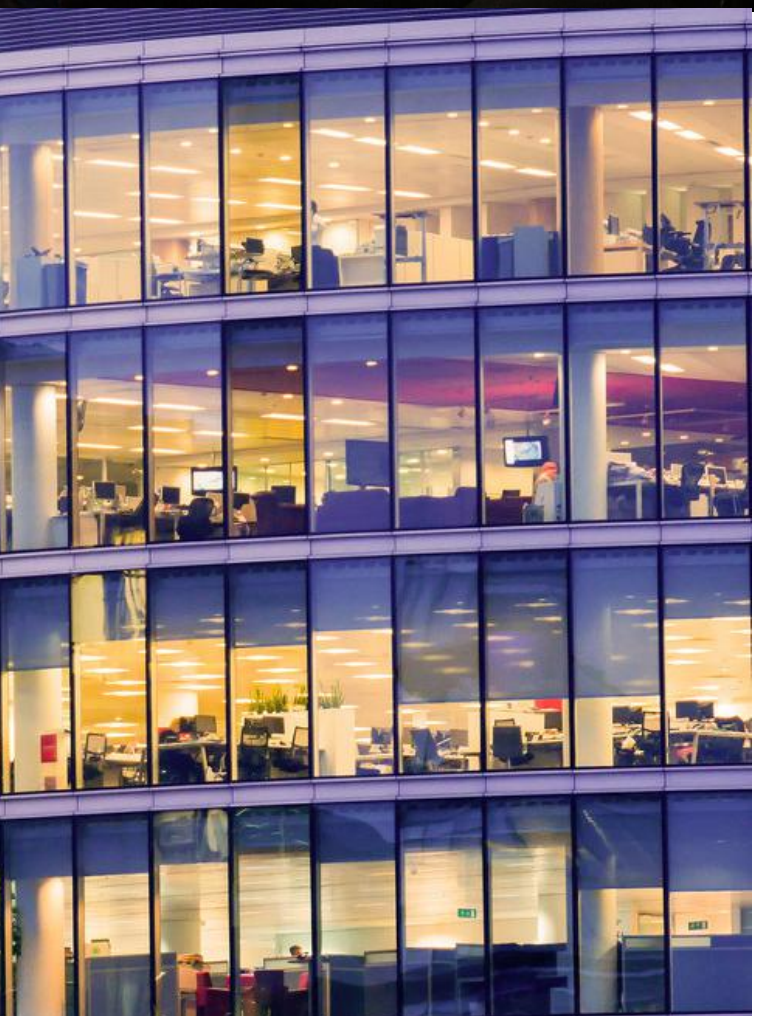
Olivia Lynch **(@Cybrary_Olivia)** is the Marketing Manager at Cybrary. Like many of you, she is just getting her toes wet in the field of cyber security. A firm believer that the pen is mightier than the sword, Olivia considers corny puns and an honest voice essential to any worthwhile blog.

CYBER SECURITY NEWS
Top headlines from the industry. All the detail you need, nothing you don't 1-4

HOT ON CYBRARY
Expolore the latest and greatest apps, courses, and content added to the site 6-7

CAREER ROADMAP
Gain insights on the most in-demand jobs in the industry and training you can use to attain them 9-10

MAKING CONNECTIONS



CYBER SECURITY NEWS

#UNLOCKED

Has Cellebrite cracked the case of the uncrackable iPhone? That's what the FBI is claiming in wake of the privacy debate over whether or not government agencies should be granted access to a suspect's locked phone.

Those who follow the news may recall the San Bernadino shootings that ignited this discussion in which the FBI infamously broke into the iPhone 5C of the terrorist in order to make their case. Although the public was unaware at first, it was later revealed that Cellebrite was, in fact, responsible for unlocking the device. Reports indicate that this service cost close to $1,000,000 and involved a system that was only successful on some phones. It seems that now, Cellebrite extended the range of phones it is capable of unlocking. The

company's marketing materials state: "Devices supported for Advanced Unlocking and Extraction Services include: Apple iOS devices and operating systems including iPhone, iPad, iPad mini, iPad Pro, and iPod Touch, running iOS 5 to iOS 11. Google Android devices, including Samsung Galaxy and Galaxy Note devices, popular devices from Alcatel, Google Nexus, HTC, Huawei, LG, Motorola, ZTE, and more."

To use their service, you have to send the device to the Cellebrite office. While there's no 100% guarantee they can unlock any phone, it has many asking if Cellebrite has an exploitable vulnerability that neither Apple not the community at large has discovered?

Want advice for protecting your privacy? Read 'How to Protect Your Online Privacy.'

#COMPLIANCE

Apple is being awfully accommodating to China. The Big 'A' just agreed to open a new Chinese data center next month which will store iCloud data and encryption keys for Chinese users in order to comply with the country's controversial data protection law.

As a reminder, China passed a Cyber Security Law in 2017 that requires 'critical information infrastructure operators' to store Chinese users' data within the country. This means that Apple must now partner with a new Chinese data center. The company, Cloud Big Data Industrial Development Co has raised many

"You can bet your boots that Cellebrite will go many miles out of its way not to let those zero-days become known, because they're the geese that lay the golden purchase orders. So, even if Cellebrite is willing to have a go at cracking phones, for a fee, your device still isn't wide open to just anyone."

-Naked Security post

concerns from human rights activists. It is important to note that this is the first time Apple will store encryption keys required to unlock iCloud accounts outside of the United States. This is especially concerning because in theory the Chinese government can "simply use their legal system to demand access to cryptographic keys required to unlock iCloud accounts stored within their nation, making it far easier to access users' data, such as messages, emails, and photos." Apple has responded that Chinese authorities will not have a backdoor into their data.

Reports indicate that Apple has not provided China with any customer account information despite receiving 176 requests from the country from 2013 to 2017. The recent decision to follow Chinese law is not the first time in recent years Apple has obliged. Last year, Apple removed VPN apps from its official Chinese App Store in China to comply with their 'Great Firewall."

"There is always the potential for government surveillance whenever encryption keys are managed by a service provider. It's not an occurrence limited to Apple or China. In the U.S. we've seen several instances in which tens of thousands of customer cloud accounts have been impacted by government surveillance requests, whether they be Apple accounts, Microsoft accounts"
-Aron Brand, CTO of CTERA Networks

For insight into the details of the Chinese Cyber Security law, read this edition of UNMASKED.

#DDOS

Sure, we hear of DDoS attacks all the time, but when a new, highly effective technique is being leveraged to commit them, it's reason for worry. This technique uses misconfigured memcached serves accessible through public Internet.

Not only is this new technique

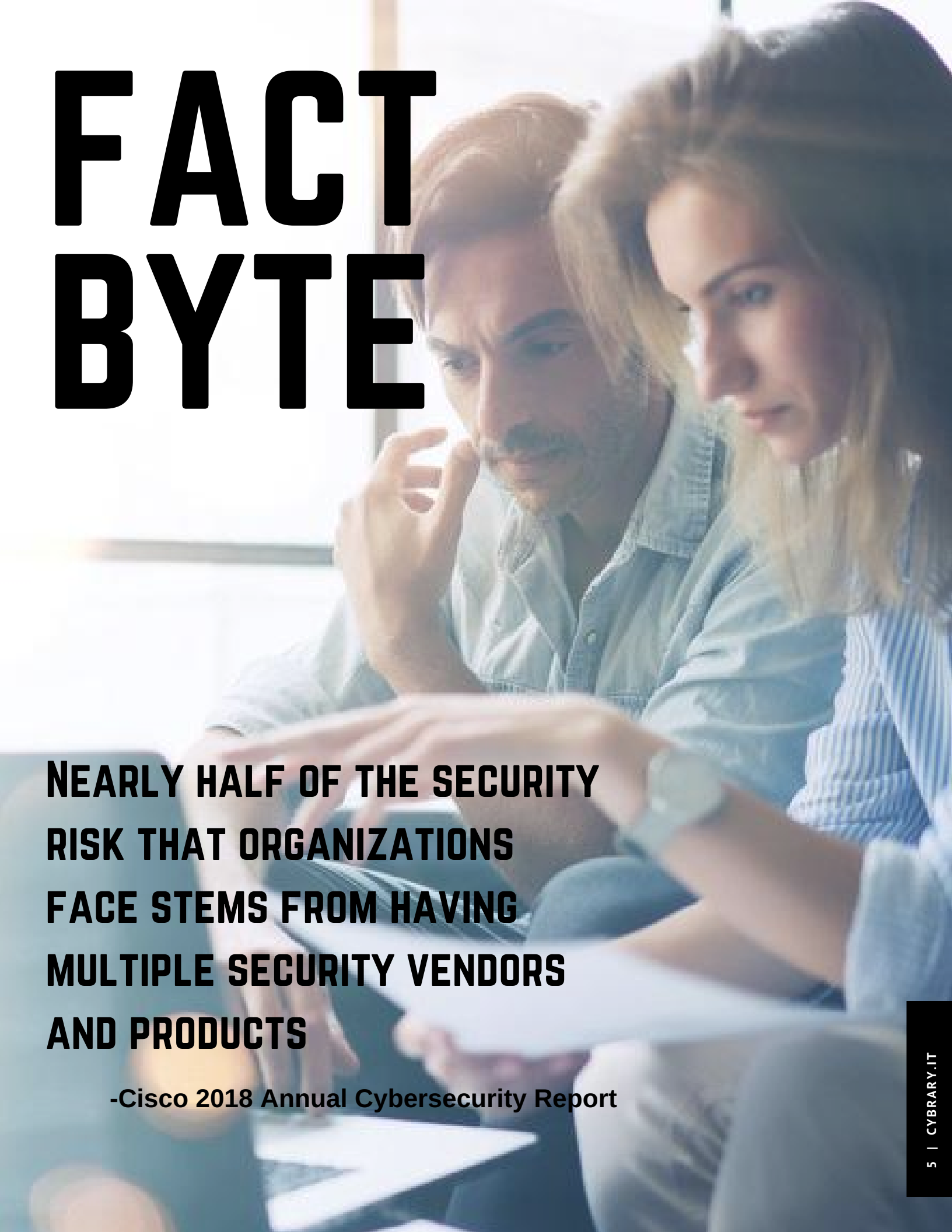
highly effective, but it also helps to simplify attacks as much as 51,200x. Reported by Akamai, Arbor Networks, and Cloudflare, the companies noticed an uptick in DDoS attacks using "User Datagram Protocol (UDP) packets amplified by memcached servers." For clarification, memcached servers are a type of server used to bolster responsiveness of database-driven websites by improving the memory caching system. In this case, attackers were able to send a small UDP-based packet request to a memcached server (on port 11211). Then, those packets would be spoofed to appear as though they were sent from the intended target of the DDoS attack.

The outcome of this type of reflection attack means that the memcache server sends the spoofed target a massively disproportionate response. “Fifteen bytes of request triggered 134KB of response. This is amplification factor of 10,000x! In practice we’ve seen a 15 byte request result in a 750kB response (that’s a 51,200x amplification),” noted a

Cloudflare researcher. What could a large scale DDoS memcache campaign mean? Because such little resources are required to carry the attacks out, the impact against intended targets as well as critical infrastructure could be great. Unfortunately, the only solution to this issue is to prevent the reflectors from being exposed to the Internet. In the meantime, organizations need to be prepared for more multigigabit attacks using this protocol and plan accordingly,” Akamai said.

Better understand how a DDoS attack works. Read 'DDoS Attack Concept Explained for Insight.'

"According to estimates, there are over 88,000 misconfigured open memcached servers vulnerable to abuse. Vulnerable memcached servers have been identified globally, with the highest concentration in North America and Europe"
-Cloudflare researchers



FACT BYTE

Nearly half of the security risk that organizations face stems from having multiple security vendors and products

-Cisco 2018 Annual Cybersecurity Report

MEET THE CYBRARIAN

Chris Greco

Chris Greco, (@grectech) a self-proclaimed Silver Hat and Senior Consultant/ trainer at GRECTECH, has almost 20 years' experience in IT. A retired Air Force Intelligence Officer and retired Federal government Civilian, Chris' background extends from public service to private industry and academia.

In his popular **'Cybersecurity for Silver Hats'** course, viewers get a series of instructional videos that help senior citizens understand the impact of cyber attacks. This course delves into the attacks and the attack vectors Black Hats use in order to get private information.

Read more

Teach on Cybrary

RMF COURSE

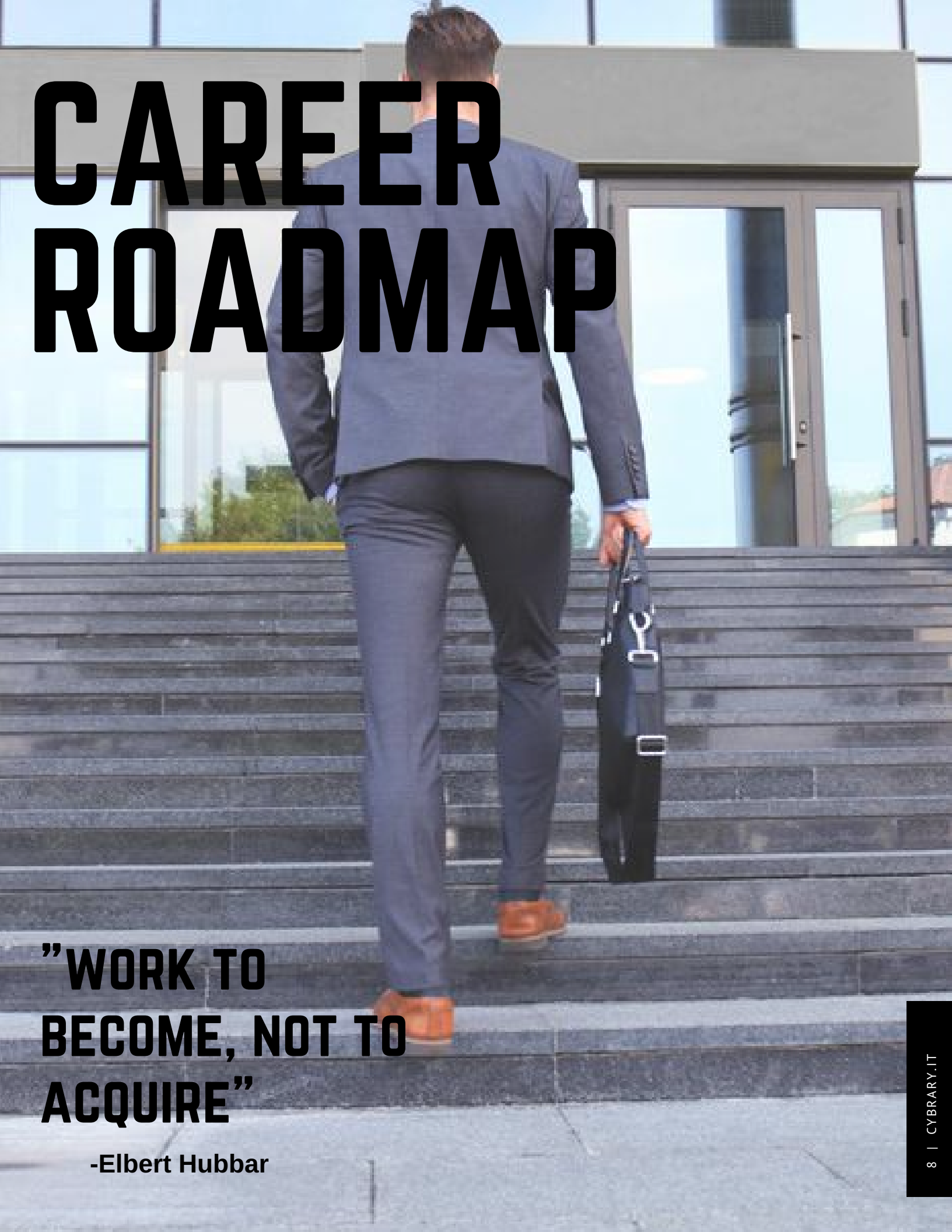
The new RMF course from Michael Redman introduces the Department of Defense (DoD) Risk Management Framework (RMF). This course prepares participants to take the CAP Exam which consists of 125 multiple choice questions and covers topics like Risk management framework, Categorization of Information Systems, and Security Control Implementation.

START COURSE

CISCO 2018 ACR ASSESSMENT

Did you capture the critical insights of Cisco's Annual Cybersecurity Report? In this interactive assessment, you can test your knowledge on the latest trends, challenges, and solutions presented in this year's report. Use code ACR2018 at checkout to take the assessment FREE and earn a Cisco badge and Certificate of Completion when you pass the assessment.

I WANT A BADGE



CAREER ROADMAP

”WORK TO BECOME, NOT TO ACQUIRE”

-Elbert Hubbar

CEH: WHAT YOU NEED TO KNOW

EC-Council's CEH course is both the oldest and most popular ethical hacking course, and for good reason — it includes 18 subject domains on both traditional hacking methods and emerging vectors such as wireless and cloud platforms along with hands-on training. The course is designed for IT pros with several years of real-world experience, and successful outcomes are improved with the addition of comprehensive study tools.

To get the full details on the CEH certification and how to study, read the rest of the popular blog.

Continue Reading **Start CEH Course**

SENIOR THREAT INTELLIGENCE ANALYST

Required Knowledge & skills

Follow the track of an industry leader's job description. Click the buttons below to view courses and supplemental materials that will put you on the path to this career

Develop and refine new threat concerns and intelligence requirements	CySA+
Create trend and correlation analysis and scenario forecasting	Threat Intel
Create and engineer systems or procedures to solve complex problems	Certified Ethical Hacker
Respond to ad-hoc vulnerability and threat-related queries	Incident Response
Support the generation of meaningful information security metrics	Malware Analysis

Career Path Beta Program

Cybrary Career Paths is a new program with the main goal of accelerating your journey to a successful technical career by providing training for technical positions with industry leaders like Cognizant.

Apply Today

MAKING CONNECTIONS

FIXING THE BROKEN HIRING SYSTEM IN CYBER SECURITY

“If you want to be a SOC manager at an organization, the platform will show you exactly what they are doing. These are the skills, and these are the average scores the team is getting, so go along this path.”

“With pure visibility into a person’s capabilities, you can vet somebody’s skills or proficiencies prior to their coming into the organization,” Corey continued.

Read the Full Post

Start a Course