

**CISO  
MAG**

beyond cybersecurity

**Internet Crime and  
Technology: Where Are  
We Headed?**

Argha Bose  
Head – Cyber Security and Risk Business  
Tata Advanced Systems Ltd.



50

COVER STORY

Volume 5 | Issue 08 | August 2021



What's next ?



NEW FRONTIERS IN  
**CYBERCRIME**




A screenshot of a Spotify music player interface. At the top left is the Spotify logo. At the top right are icons for sharing, a heart (likes), and a menu. The track title is "EPISODE #9" in bold, followed by the subtitle "Protecting 5G Networks from Sophisticated Cyberattacks". Below the text is a black and white portrait of a man with short dark hair, wearing a dark jacket. At the bottom is a playback progress bar showing "01:12" and "20:45". Below the bar are five circular control buttons: a previous track button, a previous track button, a play/pause button, a next track button, and a next track button.

A screenshot of a Spotify web player interface. At the top left is the Spotify logo. To its right are icons for sharing, a heart (likes), and a menu. The track title "EPISODE #7" is displayed in a large, bold font, followed by the subtitle "CISO Culture is All About Focusing on the Negatives" in a smaller font. Below the text is a black and white portrait of a man with short dark hair, wearing a suit jacket over a button-down shirt. The bottom of the player features a progress bar with the time "01:12" on the left and "20:45" on the right. Below the progress bar are five circular control buttons: a double left arrow (previous), a single left arrow (previous 30s), a right arrow (play/pause), a single right arrow (next 30s), and a double right arrow (next).

A screenshot of the Spotify mobile app interface. At the top, the Spotify logo is in the upper left corner. Below it, the text 'Listen Now' is displayed in a large, bold, white font. Underneath, the episode title 'How Do We Help Small and Medium Businesses with Cybersecurity?' is shown in a bold, white font. Below the title, a short description reads: 'In this episode, Brian Pereira, Editor-in-Chief, CISO MAG interviews Chris Roberts, Researcher, Hacker, and CISO, to discuss the impact of cyberattacks on small and medium businesses.' Below the text is a red 'PLAY' button. To the right of the play button are two circular icons: a heart (like) and a three-dot menu. At the bottom of the screen, a progress bar shows the current time as 01:12 and the total duration as 20:42. Below the progress bar is a row of five circular navigation icons: a double left arrow (previous), a single left arrow (previous 30s), a play button (center), a single right arrow (next 30s), and a double right arrow (next).

A black and white image of a podcast player interface. At the top left is the Spotify logo. At the top right are icons for a share symbol, a heart, and a three-dot menu. In the center is a circular profile picture of a smiling man with a shaved head, wearing a light-colored button-down shirt. Below the photo, the text 'EPISODE # 3' is displayed. The main title 'How Zoom is Enhancing Security and Evolving its Product' is written in a large, bold, sans-serif font. At the bottom, a progress bar shows '01:12' on the left and '20:41' on the right. Below the progress bar are five circular control buttons: a double left arrow, a single left arrow, a large play button in the center, a single right arrow, and a double right arrow.

Listen to the podcasts exclusively on

The Spotify logo, consisting of a green circular icon with three horizontal white lines and the word "Spotify" in white, is centered below the text.

The image features a black background. In the upper left, there is a red square logo with a white border containing the text "CISO MAG" in white, with "beyond cybersecurity" in smaller white text below it. To the right of this is a red microphone icon with white sound waves above it, and the word "PODCAST" in white capital letters below the microphone. Centered in the lower half of the image is the text "LISTEN TO THE LATEST CYBERSECURITY TRENDS AND INSIGHTS BY POPULAR INDUSTRY LEADERS ON THE GO." in white, bold, sans-serif capital letters.



 Spotify

## Intel Labs' Breakthrough Research on Data Privacy and Encryption Technologies

In this episode, researchers from Intel Labs in the U.S. explain how Federated Learning and Homomorphic Encryption is driving new applications that require secure data sharing and data privacy

**PLAY**

A screenshot of a YouTube video player. The video title is "The Case for Virtual Cybersecurity" and it is labeled as "EPISODE #10". The video is from the channel "Spotify", indicated by the logo in the top left. The video features a man with glasses and a light blue shirt. The video progress bar shows the video is at 01:12 out of 04:42. The video player controls at the bottom include a play button, a volume icon, and a full screen icon.

Listen to the podcasts exclusively on

The Spotify logo, consisting of a green circular icon with three horizontal white lines and the word "Spotify" in a green sans-serif font with a registered trademark symbol.

A screenshot of a Spotify podcast player interface. At the top left is the Spotify logo. At the top right are icons for sharing, heart, and a menu. In the center is a circular profile picture of a man with glasses. Below the picture, the text 'EPISODE # 11' is displayed. The main title 'Supply Chain Attacks and Vulnerability Disclosures' is shown in a large, bold font. At the bottom, there is a progress bar with the time '01:12' on the left and '20:41' on the right. Below the progress bar are five circular control buttons: a previous episode button (double left arrow), a previous episode button (single left arrow), a play button (triangle), a next episode button (single right arrow), and a next episode button (double right arrow).

A screenshot of a Spotify podcast player. At the top left is the Spotify logo. At the top right are icons for share, heart, and a menu. The title "EPISODE #1" is centered, followed by the subtitle "How Digital Risk Management (DRM) is Changing During the Pandemic". Below this is a black and white portrait of a man with glasses, wearing a suit and tie. At the bottom is a progress bar showing "01:12" and "21:40". Below the bar are five circular control buttons: a previous track button, a previous track button, a play/pause button, a next track button, and a next track button.

Spotify

PLAYLIST

# CISO MAG

Playlist description  
Created by **Podcast Channel**

Search

PLAY

Download

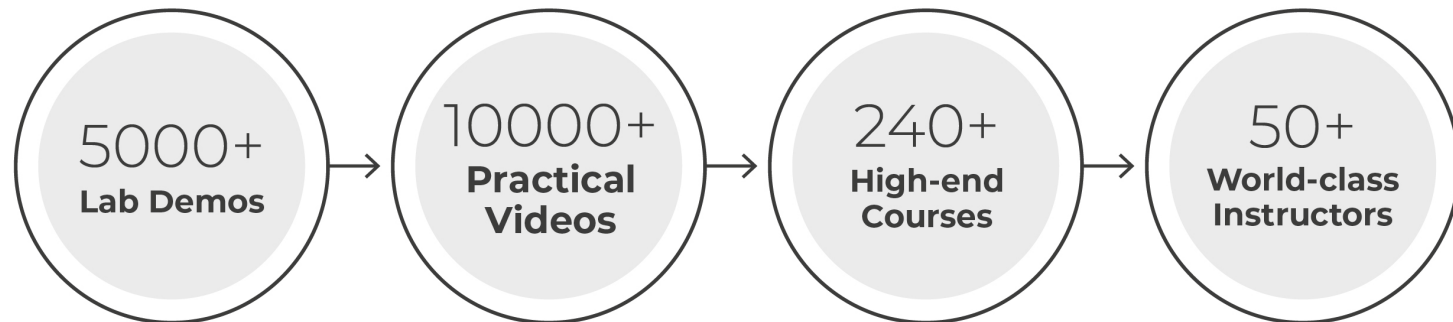
	TITLE	
♥	EPISODE #8	21:40
♥	EPISODE #9	20:45
♥	EPISODE #10	20:41
♥	EPISODE #11	20:41
♥	EPISODE #12	23:13
♥	EPISODE #13	21:44
♥	EPISODE #14	20:45

A Spotify player interface on a dark background. At the top left is the Spotify logo. The main title 'Listen Now' is in large white font. Below it, the episode title 'CISO Culture is All About Focusing on the Negatives' is displayed in white. A description follows: 'In this episode, Adam Palmer, Chief Cybersecurity Strategist, Tenable, explains cybersecurity metrics and the CISO culture of focusing on the negatives.' Below the text is a red 'PLAY' button. To the right of the button are two circular icons: a heart and a three-dot menu. At the bottom, a progress bar shows '01:12' on the left and '20:42' on the right. Below the progress bar are five circular control buttons: a previous track button, a play/pause button (which is highlighted with a white border), a next track button, and two additional buttons for full screen and a share menu.

## LEARN EVERYTHING THERE IS TO KNOW ABOUT **CYBERSECURITY.**



Master in-demand cybersecurity skills online with unlimited access to all of our premium videos and demo labs curated from our hand-picked global experts



### Browse Courses in Your Favorite Categories



Secure Programming



Data Science



Information Security



Network Security



Cloud Computing

### Learn faster with courses built just for you!

With our state-of-the-art Machine Learning and deep data analytics, we are able to recommend courses to you based on your career goals and watch history, so you can see progress in your career faster than ever without being overwhelmed by too many choices of what to learn next.



Track your performance



Set daily goals



Personalized support

### Practical Content for Practical People

As always, with all EC Council products, we put practical knowledge over everything else! With more than 5000 lab videos that goes in detail on how you can perform each single task in the course, you will be able to truly master new skills, not by just hearing about them but by practicing them.



Add lessons to  
your favorites list



Add and save notes  
on your lessons



Exercises files and  
external resources

### Show Off Skills With Our Industry-Leading Certificates

Once you complete any of our CodeRed Pro courses, you will receive a "certificate of achievement" from CodeRed and EC Council that you can share with your employers and community.



You're One Step Away From Starting  
Your Learning Journey with CodeRed

Use Coupon code **CISO30**  
to get exclusive **30% off on your subscription.**

**Start Learning Today!**





# WEB APPLICATION HACKING AND SECURITY

**100% Hands-On | Lab-Based**

*From the team that brought you the  
Certified Ethical Hacker*

Become A  
**Certified Web Application**  
**Associate | Professional | Expert**



## WHY

**Is It Important?**

**Application security is one of the fastest growing cybersecurity skill<sup>1</sup>**

If you are tasked with implementing, managing, or protecting web applications, then this course is for you. If you are a cyber or tech professional who is interested in learning or recommending mitigation methods to a myriad of web security issues and want a pure hands-on program, then this is the course you have been waiting for.

**Get Certified Today**



<https://www.forbes.com/sites/louiscolombus/2020/11/01/what-are-the-fastest-growing-cybersecurity-skills-in-2021/>

## HOW

**You Will Learn?**

Unlike many Capture-the-Flag challenges and Vulnerable Virtual Machines, Web Application Hacking and Security provides the challenger with the ability to follow an instructor as they make their way through the challenges. The instructor will present alternatives, do scans, upload malicious payloads, and crack passwords from their home computer just like you. – But don't rely on the walkthrough; challenge yourself and see how far you can get. Play some of the walkthroughs, then pause and try some more.

Beginner

Intermediate

Proficient

Expert

Break The C</>DE

**REGISTER NOW**

## WHAT

**You Will Learn?**

- Advanced Web Application Penetration Testing
- Advanced SQL Injection (SQLi)
- Reflected, Stored and DOM-based
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF) – GET and POST Methods
- Server-Side Request Forgery (SSRF)
- Security Misconfigurations
- Directory Browsing/Bruteforcing
- CMS Vulnerability Scanning
- Network Scanning
- Auth Bypass
- Web App Enumeration
- Dictionary Attack
- Insecure Direct Object Reference Prevention (IDOR)
- Broken Access Control
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Arbitrary File Download
- Arbitrary File Upload
- Using Components with Known Vulnerabilities
- Command Injection
- Remote Code Execution
- File Tampering
- Privilege Escalation
- Log Poisoning
- Weak SSL Ciphers
- Cookie Modification
- Source Code Analysis
- HTTP Header modification
- Session Fixation
- Clickjacking

Level up your skill







Volume 5 | Issue 08  
August 2021

President & CEO  
**Jay Bavisi**

#### Editorial

Editor-in-Chief  
**Brian Pereira\***  
brian.p@eccouncil.org

Sub Editor  
**Pooja Tikekar**  
pooja.v@eccouncil.org

Sr. Technical Writer  
**Mihir Bagwe**  
mihir.b@eccouncil.org

Sr. Feature Writer  
**Rudra Srinivas**  
rudra.s@eccouncil.org

#### Management

Senior Vice President  
**Karan Henrik**  
karan.henrik@eccouncil.org

General Manager - Marketing  
**Seema Bhatia**  
seema.b@eccouncil.org

Senior Director  
**Raj Kumar Vishwakarma**  
rajkumar@eccouncil.org

Head - Research & Content  
**Jyoti Punjabi**  
jyoti.punjabi@eccouncil.org

Publishing Sales Manager  
**Taruna Bose**  
taruna.b@eccouncil.org

Manager - Digital Marketing  
**Rajashakher Intha**  
rajashakher.i@eccouncil.org

Asst. Manager Visualizer cum Graphic Designer  
**Jeevana Rao Jinaga**  
jeevana.r@eccouncil.org

Manager - Marketing and Operations  
**Munazza Khan**  
munazza.k@eccouncil.org

Image credits: Shutterstock & Freepik  
Illustrations, Survey Design, Cover & Layouts by: Jeevana Rao Jinaga

\* Responsible for selection of news under PRB Act. Printed & Published by Brian Pereira, E-Commerce Consultants Pvt. Ltd.,  
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.

## EDITOR'S NOTE

# GHOST IN THE MACHINE

As I write this note in late July, the most trending cybersecurity news is the Pegasus Spyware incident. This isn't the first time we've heard about Pegasus; remember the 2019 incident where Pegasus was infecting phones through WhatsApp? However, the issue garnered a lot of importance this time as journalists, activists and politicians are also affected with spyware. In India, the news of Pegasus caused mayhem and disruption as the monsoon session of Parliament began; politicians accused the government and opposing political parties of snooping on their phone messages and conversations. The phone numbers of senior Indian journalists are also on the dreaded Pegasus surveillance list, making them possible victims of spyware. So, who's the real culprit then?

The Israeli NSO Group Technologies, which created Pegasus spyware, has vehemently denied any involvement. It says it just creates this tool and sells it to governments and intelligence or security agencies. NSO says it cannot be held accountable for how its customers use this tool. So, the licensees should be held responsible. But then, there is a thin line between surveillance and snooping. Who decides what is legal and permissible and what violates one's privacy?

This incident also raises a few questions:

- Is it possible to get infected by spyware without clicking on any links (zero click)?
- Can someone plant spyware on your phone just by knowing your number?
- How does one know if they have been infected by Pegasus spyware?
- And how do you remove this spyware from your phone?

I am hoping the answers to these questions will emerge soon. Because if it doesn't, a lot of people may get paranoid.

Well, attacks on our personal space show the extent to which threat vectors have evolved.



**Brian Pereira**  
Editor-in-Chief

Argha Bose, Head – Cyber Security and Risk Business, Tata Advanced Systems Ltd., sums it up well in the Cover Story that he wrote for this issue. He writes, "...the world is transforming into a network of objects that are constantly gathering personal and sensitive information across various areas of their deployment, and the lack of security measures on them could lead to a catastrophe." Read his article on [page 50](#).

Ransomware attacks are so common today, and now we even have Ransomware-as-a-Service. The Kaseya ransomware attack by the Russia-linked REvil Group hit small and medium businesses hard. It also taught us a thing or two. Can we proactively check the compliance and risk posture of everyone in our supply chain and at ALL levels? Our Sub Editor, Pooja Tikekar, reports on the Kaseya ransomware incident in Buzz on [page 20](#).

They say that if there was no cryptocurrency, there would be fewer ransomware attacks. However, with cryptocurrency gaining popularity since the beginning of the pandemic and now reaching a market capitalization of nearly \$2 trillion in Q1 2021, a subsequent rise in the number of cryptojacking incidents has been recorded. And Monero cryptocurrency is most favored by threat actors for their illicit mining activities, reports our Sr. Technical Writer, Mihir Bagwe, on [page 68](#).

Zachery S. Mitcham, VP and CISO, SURGE Professional Services-Group, explains how cryptojacking works and also recommends some mitigation measures in Knowledge Hub on [page 60](#).

We hope you enjoy reading the articles in this issue.



# Contents

## OPINION

**Cybersecurity –  
The Path of Most  
Resistance**

12

## BUZZ

**Kaseya®**

**RANSOMWARE**

**How REvil Paralyzed  
Kaseya VSA in  
a Supply Chain  
Ransomware Attack**

20

## UNDER THE SPOTLIGHT

**Speed is the  
Reason Why 1  
In 3 Employees  
Do Not Use VPN**

**Anthony Di Bello**  
VP of Strategic Development  
OpenText

34

## INSIGHT

**Rise in RAT  
Campaigns  
Illustrates Growing  
Malware Threat**

42

## COVER STORY

**Internet Crime and  
Technology: Where Are  
We Headed?**

50

## KNOWLEDGE HUB

**Cryptojacking –  
The Parasitic Cybercrime**

60

## TABLE TALK

**Until now, technology  
gave you no protection  
and confidentiality  
when you shared your  
data**

**Richard Gendal Brown**  
CTO  
R3

74

**REWIND**

84



# Cybersecurity – The Path of Most Resistance



**Dick Wilkinson**  
Chief Technology Officer  
New Mexico Judicial Information Division



In a very short timeline, computers and electronic technology have drastically changed the way humans live. We have welcomed these devices into our lives to increase convenience and make the most of the things we do easier in our day-to-day lives. The relationship with technology has generally been a very enjoyable experience. Many people enjoy the convenience of technology so much they claim they would be lost without their cell phone, as in literally lost. However, there are some aspects of our relationship with computers that many people find an ever-increasing frustration, enter the password.

Passwords and other security features are the necessary evil we all tolerate to make sure our computer use is an enjoyable experience and not a string of random fraud and crimes happening on your cellphone or laptop. Customers find security features tolerable, not enjoyable. Customers of technology have seen a trend over the decades. The trend calls for smaller devices with fewer buttons, fewer switches, and endless physical interaction with your network or device. The user experience is becoming almost completely touchless and seamless. Voice assistants, like Alexa or Google Home, are the perfect example of what users have always wanted their computers to be: interactive, easy, powerful, and touchless. A serious problem occurs when security features of any new technology slow down the user experience, add physical touches or additional clicks, and require focus and time to make them happen exactly right, or you are locked out of your session. All these interactions are a nuisance to the user. Security has established itself as the path of most resistance in the life of a technology customer.





## The path to least resistance causes breaches

Security features are difficult to navigate and creates a problem that is often easy to overcome, enter the workaround. Humans by our nature will seek the path of least resistance to get a task done. No matter how serious or trivial the task, we expect to find or create the easiest series of steps to complete the work. Many modern jobs happen in an office with computers and the tasks become repetitive and time consuming even with the help of computers. The employees completing these repetitive tasks are always seeking the path of least resistance, and that is a good thing. You want to nurture efficiency in your company and employees be creative is a great way to find those efficient methods. That creativity quickly runs afoul of security, which is rule driven, structured, and immovable.

IT security uses rules and risk management to ensure only the right people get the right information. Security uses gates and fences and slows the path of least resistance down to your way to pass through. If you will never get to the end of the road for. The earlier the security becomes even the disconnect between the user and the perpetrator are perpetrated by a single user. A simple security policy that must be created.

## Barriers to security

One gate was not enough, we have now introduced multiple gates that require multiple "keys" to pass. That is the exact opposite of what a user wants; they want zero passwords, not extra passwords to make sure the first password works properly. People are smart and have realized that passing through the digital gate is only one option, you can also jump over the fence.

An employee is working with a customer who needs to receive several large files. The employee has to make it through your corporate security because they have realized that there are also other ways to get the files.

**SUBSCRIBE NOW**

TO READ THE FULL ISSUE