Rotary Club of Charlotte

THIS WEEK'S PROGRAM

March 15, 2022

2021- 2022 Board Members

President Carol Hardison
Pres Elect William Bradley
Past Pres Jerry Coughter
Secretary Colleen Brannan
Treasurer Edwin Peacock
Exec Sec Christine Cipriano

Directors 2021-2022
Patrick Baker
Bill Bartee
Suzanne Bledsoe
Kim McMillan
Rex Reynolds
Ranjay Sarda
John zumBrunnen

Directors 2021-2023
Ann Clark
Ellison Clary
Jesse Hite
Warren Kean
Vanessa Stolen

Membership Laura Little

Foundation Joe Morris

Programs Elly Clary

Andrew Travis:

What is Ransomware?

By Suzanne Bledsoe

Andrew Travis, a Charlotte newcomer, is a systems engineer at Fortinet, covering the Charlotte area and South Carolina. A graduate of Virginia Tech, he focuses on designing software solutions to improve the security of information systems. He shared with us some of the ways that our use of everyday technology can lead to unintended and costly consequences.

Cybercriminals have become very adept at hacking into computer systems, capturing and blocking access to data, and disrupting business operations. Ransomware is a form of malicious software, or malware, which, once installed on a computer, locks and encrypts the device, thereby blocking access to personal files, or more importantly, data necessary to normal business operations. In order to restore access and unlock the files, a ransom must be paid. Cybercriminals exploit weaknesses in security systems, through a variety of tactics such as embedding malware in email attachments or links to websites. The cost to restore systems, once the malware is installed, is significant, regardless of whether the ransom is paid.

There are a variety of processes and procedures that help protect against vulnerabilities associated with a ransomware attack. Organizations should develop and maintain a written plan that identifies a systems management and recovery team, requires periodic risk assessments and creates and conducts or oversees disaster recovery plans. Cybersecurity insurance is a common form of risk management and cost containment for many organizations, particularly those that are most vulnerable to attack. Education of employees and stakeholders is critical; virtually any user of a device connected to a larger system can inadvertently trigger malware that creates an opening into the larger system.

The incidents of ransomware attacks have escalated significantly since they were first detected in 2005. Cybercriminals are more sophisticated and have

developed well-defined processes for identifying and exploiting vulnerable systems. The cost of recovery from ransomware incidents in 2021 was $20B, and is expected to be as much as $265B in 2031. In addition to steep recovery costs, losses due to business interruption, and potential exposure of sensitive data, reputational risk is also significant.

So, the next time you are intrigued by the odd email, attachments, or website links, think twice before clicking—it could the gateway to a world of hurt!

Thanks to Andrew for the warning.

*A recording of the program is available here: https://vimeo.com/688870569
Mr. Travis' introduction begins at 16:10 minutes.