June 20, 2020

Mesa, AZ

Ransomware as a Service …yes, you read correctly! Attacks are growing. Hackers are more blatant. So brazen that they need help and are hiring! The dark web is now the recruiting tool. Hackers need help collecting the money while they move onto setting up the next attack. Think of it as admin help or the accounting function.

This quote from the NY TIMES February 2020 shows that Small and Medium Size Businesses (#SMB) are vulnerable and need to be vigilant.

"Ransomware attacks have also caused a number of small and medium businesses to shut altogether, like Colorado Timberline, a printing company with a few hundred employees near Denver, and Brookside ENT and Hearing Services in Battle Creek, Mich., a 10-person medical office.

"I was suddenly retired and I didn't want to be," said Dr. William Scalf, one of two doctors at Brookside, which closed in April after failing to recover its medical files from hackers who demanded $6,500."

$6500 was all it took to close down a medical office.

So how do you stay vigilant? Osama Tahir's recent blog quotes several thought-leaders and cyber security experts including Al Marcella, CISA, CISM in the need for employee training and what to include in an effective training program. Tahir sites this statistic, which shows that organizations are not protecting themselves from today's largest threat to business.

According to a report published by Chubb, only **31%** of the employees surveyed reported to have received company-wide cybersecurity education and training.

Read Tahir's BLOG.

ABOUT Madeline Parisi & Associates LLC

We help organizations stay in business given today's world of cyber threat opportunities by understanding risk, and knowing how to manage and mitigate risks. We guide organizations with training and comprehensive written training materials to identify threat actors and malicious activities like ransomware, and how be alert to scams that have impacted many businesses large and small. A key component to accomplishing internally is leadership and communication. Being vigilant is a top-down process. Training includes face-to-face when available. Content includes:

- Cybersecurity
- Risk Management and Risk Mitigation
- Managing (or Starting) a Compliant Commercial UAS (drones) Prrogram
- Leadership
- Interest-based Leadership (Communication)
- Audit and Security Study Materials