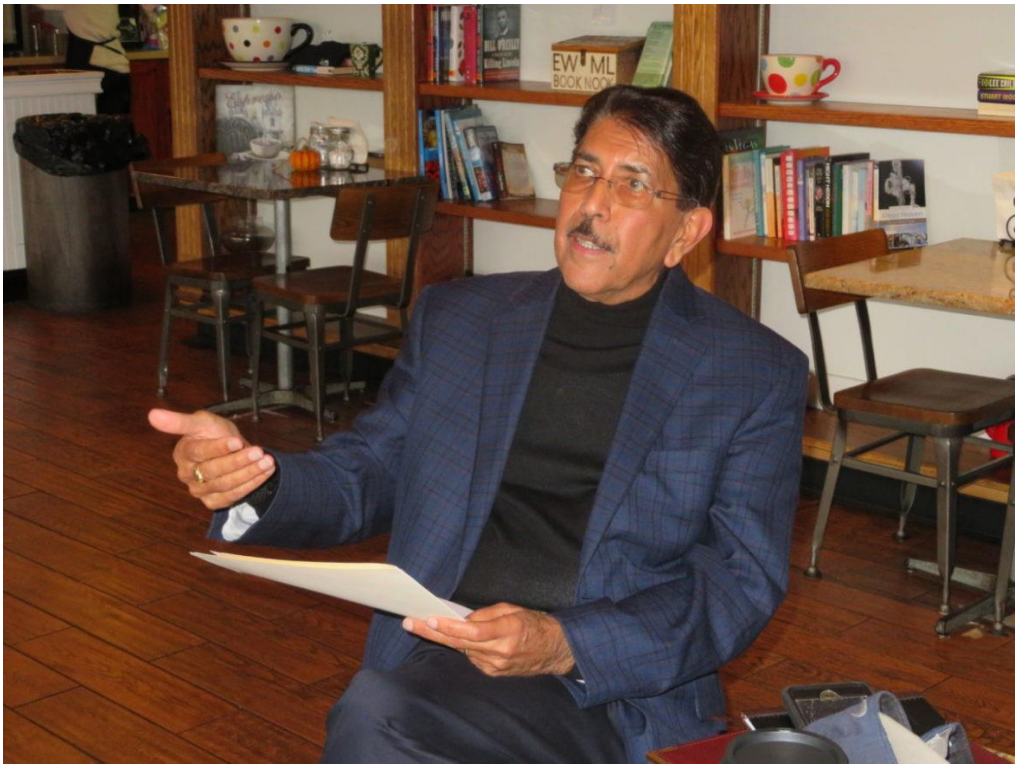
The Monroe Sun
Shining a light on the news of our town.

https://themonroesun.com/cybercriminals-can-put-you-out-of-business-in-a-heartbeat/

Cybercriminals can put you out of business in a heartbeat

By Bill Bittar

Oct. 19, 2020



https://themonroesun.com/

Arvin Chaudhary, of Monroe, is founder and president of Nadicent Technologies. He explains the dangers of cybercrime during an interview at Last Drop Coffee Shop on Main Street in Monroe Friday.

MONROE, CT — Arvin Chaudhary wore a face mask while entering Last Drop Coffee Shop for an interview Friday afternoon, and pushed his seat back further from the table to comply with social distancing measures meant to stem the spread of the coronavirus.

Chaudhary, of Monroe, is just as careful when following measures to foil online criminals trying to hack into the files of his clients. He is founder and president of Nadicent Technologies and one of its specialities is cybersecurity.

A successful cyberattack can deal a significant blow to a large company's finances, productivity and reputation — and small companies are not spared from the threat, Chaudhary warns.

"You may think, 'I'm so small, no one wants me,'" he said. "They can get you out of business in a heartbeat. An individual can steal your I.D. and clean out your bank account."

October is Cybersecurity Awareness Month, and Chaudhary took some time to share steps businesses and individuals can take to protect their data, systems and finances.

It is estimated that cybercrime damages will cost $6 trillion globally by 2021 and ransomware damage costs are predicted to be 57 times higher in 2021, reaching $20 billion compared to 2015, according to Nadicent.

"Everyone is working remotely," Chaudhary said. "Everyone is exposed. The hackers are very much geared up to take advantage of this. A company of 100 employees went from one to 100 locations."

He said ransomware is up 800 percent and phishing is up around 500 percent, adding, "the threats are incredible and you're much less protected."

Finding the right fit

Chaudhary's experience includes 20 years in various roles for Hewlett Packard/Agilent, most recently as vice president and general manager, leading HP's Worldwide Wireless Services Division.

"I ran a division running wireless services and caller networks," he recalled. "After 9/11, a corporate mandate called for significant downsizing."

Chaudhary said the challenge for his division was, "how do we change our business model to allow us to serve our customers and still grow our business?"

He said they came up with a plan to have teams of five engineers, with one being the lead engineer. The teams worked with subcontractors. "We were able to convert all our fixed costs to variable costs and save their jobs, while reducing head count," Chaudhary said.

He brought the same system to his own business, Nadicent Technologies, which he founded in 2003. The company will soon be moving from Glastonbury to Shelton.

Nadicent specializes in cybersecurity, mobility, the cloud, and telecommunications. Nadicent, which has a team of 100 people, works directly with its clients to assess their needs. Then it uses its expertise and large portfolio of over 200 vetted suppliers to find the best contractor for the job.

“We know the market,” Chaudhary said of narrowing searches. “Now the customer has the competitiveness and the suppliers are happy.”

This saves a business significant time over assigning its own employees to do all of the research and interviews to narrow everything down to a shortlist of the best candidates.

“What could take a year, we could do in two months,” Chaudhary said. “We are the river connecting the mountains and the oceans.”

Nadi means river in sanskrit and cent means 100, Chaudhary said of his company’s name.

A cautionary tale

Chaudhary said the four countries who are most active in cybercrime are China, Russia, North Korea and Iran. One of the most common attacks is tricking people into clicking on links that download ransomware on their computer, which then can be used to infect others.

Ransomware is a form of malware that encrypts a victim’s files, locking users out of their computers. Chaudhary said you could encrypt your files to prevent theft of your data, but hackers can still add a layer of encryption over it preventing you from accessing it too.

The attacker then demands a ransom from the victim to restore access to the data upon payment, which can escalate every day it goes unpaid. The FBI recommends not paying, because it can embolden the attackers.

In 2017, Erie County Medical Center in Buffalo was hit with a massive cyberattack that brought down the hospital’s computer systems. The thieves demanded $30,000. ECMC officials estimate expenses tied to the incident were nearly $10 million, according to an article in The Buffalo News.

Chaudhary said much of the cost was in replacing all of the hospital’s computers. According to The Buffalo News, “medical center officials also anticipate an ongoing additional expense of $250,000 to $400,000 a month for investments in upgraded technology and employee education to harden its computer system defenses to reduce the risk and impact of future attacks.”

“Most often, companies are attacked through their weakest link: Their employees or suppliers,” Chaudhary said, adding children of employees working from home could pose another vulnerability when they go online.

He said 90 percent of cyberattacks start with phishing, or social engineering. A friend's computer could be compromised and the hacker will use their email list to send messages to entice you to click on a link.

Chaudhary said clicking on it could download ransomware or a trojan horse that allows criminals to read everything on your computer, including passwords.

"If malware is sitting on your computer, someone can log in as you and remotely control the inside of a corporate building," he said.

How to protect yourself

When it comes to protecting your business from cybercrime, knowledge is power. Chaudhary said Nadicent offers employee training to raise awareness, helping employees to recognize and avoid clicking on suspicious links.

"Cyber awareness is the lowest cost and highest possible return," Chaudhary said.

Many scams are also carried out over the phone.

When the U.S. Small Business Administration offered Paycheck Protection Loans, Chaudhary said cybercriminals knew banks would be calling businesses who applied, to take down sensitive information, such as Social Security or employer identification numbers.

"Your business is suffering. You're looking for a loan and someone calls saying, 'I'm with Bank of America and I want to talk about your loan,'" Chaudhary said.

While you may be tempted to start talking, Chaudhary said you should ask questions first. "I don't know you. You could be a hacker. How much money did I apply for? When did I apply?"

"They will hang up," he said.

Spoofing is something else to watch out for. This is when cybercriminals send a message like, "we saw some activity on your bank account," along with a link to take you to your bank's page to sign into your account to find out what's going on. The page is made to look like your bank's page and it is a way to steal your username and password.

"You shouldn't need a link to go to your bank's homepage and sign into your account," Chaudhary said.

Typo-squatting is another online threat, according to Chaudhary. This is when cybercriminals establish web addresses that are similar, sometimes just one letter off, to legitimate websites. By doing this, victims can end up on their site, simply by making a typo.

He said some companies will purchase domains that are similar to theirs, so cybercriminals cannot purchase one that is one character off to fool clients.

Low to no cost solutions

Nadicent has an advisor security center anyone can access with news and alerts on the latest scams. Here's a link. Chaudhary also has a podcast on his company website. He recommends visiting the Federal Trade Commission's page on protecting American consumers as another way to stay in the know.

Here are other tips Chaudhary shared:

Don't click on phishing emails, spoofed emails and websites.

Use strong, long, non-guessable passwords and change them every three to six months.

Chaudhary said it is important to change them, because companies are being compromised by hackers all the time and your information could be in those files. To find out if you were compromised by a data breach, visit http://haveibeenpwned.com/.

To avoid having to constantly memorize new passwords, Chaudhary recommends using a password manager like Roboform, Lastpass or 1password.

Add dual authentication to critical accounts, such as email, financial and buying sites. Add a PIN to your cellphone account.

Update software regularly — Apple, Microsoft etc., update for security and additional features.

Install good antivirus software on your PC, MAC, iPad/Tablet, Smartphone etc. (Norton/Lifelock, McAfee, Cylance, SentinalOne).

Use Adblock – free or $10 a year on the browsers, use a different browser or Chromebook or critical accounts if really paranoid.

When using public WIFI at restaurants, hotels, etc., use VPN.

Back up your data and disconnect the drive. Encrypt your computer drive – save the key, have a cloud backup.

Monitor credit reports, use identity protection like Norton or LifeLock. Advanced: Use IOT Protection, cloud based security rather than a firewall on the site.