https://www.nhregister.com/business/article/Today-s-Business-7-myths-small-business-owners-16174277.php

New Haven Register

https://www.ctpost.com/business/article/Today-s-Business-7-myths-small-business-owners-16174277.php

CONNECTICUT POST

https://www.middletownpress.com/business/article/Today-s-Business-7-myths-small-business-owners-16174277.php

The Middletown Press

https://www.thehour.com/business/article/Today-s-Business-7-myths-small-business-owners-16174277.php

The Hour

https://www.stamfordadvocate.com/business/article/Today-s-Business-7-myths-small-business-owners-16174277.php

sa stamford advocate

https://www.newstimes.com/business/article/Today-s-Business-7-myths-small-business-owners-16174277.php

newstimes.com

https://www.greenwichtime.com/business/article/Today-s-Business-7-myths-small-business-owners-16174277.php

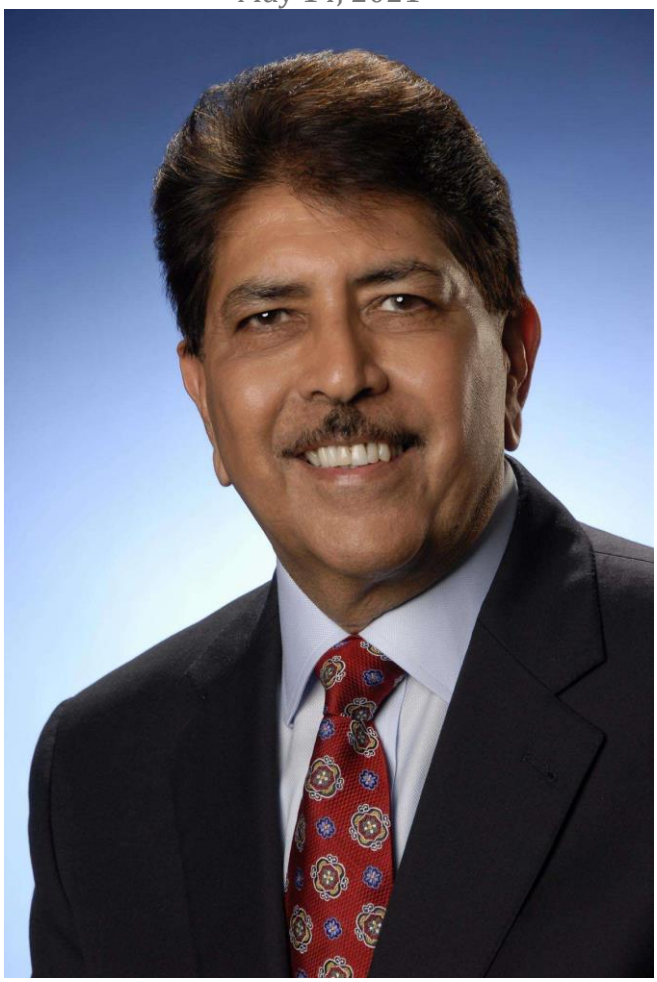
gt greenwich time

https://www.registercitizen.com/business/article/Today-s-Business-7-myths-small-business-owners-16174277.php

THE REGISTER CITIZEN

# Today's Business: 7 myths small-business owners need to ignore

Arvin Chaudhary
May 14, 2021



Arvin Chaudhary Contributed photo

Ransomware and other cyberattacks long have been a challenge for small businesses. However, the recent shutdown of Colonial Pipeline has raised significant concerns for small businesses and the White House alike.

Small businesses are least protected and most attacked — 60 percent go out of business within six months after being breached since 83 percent do not carry cyber insurance.

A small business can significantly improve its cybersecurity quickly and affordably. However, first consider these misconceptions and myths:

**1. I am too small to be hacked**

Incorrect. There was a 424 percent increase in new small-business cyber breaches last year. According to Verizon, 28 percent of data breaches in 2020 involved small businesses.

**2. Installing antivirus software on my computers is enough**

No. Antivirus software is helpful but not sufficient to protect against hundreds of thousands of new malware appearing daily. Expect that the antivirus protection will fail. Computers and servers must be backed up and tested for recovery if a ransomware attack cripples computers.

**3. Cyberattacks come from external sources only**

Not true. Insider threats also pose risks. Insider threats can stem from an employee or even someone whom your company once employed. An insider can intentionally download a company's sensitive data or inadvertently insert an infected USB memory stick in one of the firm's computers.

**4. My IT department will take care of everything**

With new threats appearing daily, it would be foolhardy to put all your cybersecurity responsibility on your IT team. More than 90 percent of breaches start with phishing (email, text, etc.). Hence, cybersecurity awareness training for the employees is an inexpensive way to reduce the threats.

**5. My business is 100 percent protected from cyberattack**

Cybersecurity is something that you never stop working to improve. Threats evolve constantly. With millions of dollars in cybersecurity investments, companies such as Target and Home Depot got hacked through vulnerability in their supply chains or suppliers' weak security. The pandemic forced small

businesses to have employees work from home — without implementing proper cybersecurity for remote workers.

**6. We don't need to use a password manager or two-factor authentication**

About 60 percent of data breaches happen due to weak or reused passwords. Most people have 50-100 business and personal accounts online. It is impossible to remember that many unique, 14-plus-character passwords.

As a result, people tend to reuse simple passwords or write them on paper. Instead, use inexpensive, easy-to-use password managers. The user only needs to remember one long master password and the password manager remembers the rest.

Setting two-factor authentication on critical accounts (email, financial, etc.) is free and easy to implement, perhaps with initial guidance from the IT folks. With TFA, the email or bank will send you a 6-digit code to enter when you log in.

**7. Cyber liability coverage is too expensive**

Small businesses go out of business due to the high costs of recovering from a breach. A company should have sufficient insurance coverage for ransomware, compliance failure, business income loss and cyber legal liability. Cyber insurance is expensive, and the underwriting is complicated. However, purchasing cyber protection bundled with cyber liability can make it affordable.

Since the sensitive information resides on computing devices (laptops, computers and servers), those devices need to be well secured. Even a small business with ten devices can get robust device security (protect, detect and respond) for about $250 per month, including about $500,000 in liability protection.

In summary, to minimize cyber threats and resulting disasters, a business should at least implement free cybersecurity awareness training for the employees (see FTC.gov and CyberReadinessInstitute.org), use a password manager and two-factor authentication, regularly back up the computers, and get good cybersecurity protection for the devices, including cyber liability coverage.

*Arvin Chaudhary is chief executive officer of technology services company Nadicent Technologies. He can be reached at Arvin.Chaudhary@Nadicent.com or 203-274-8466. Free email alerts about scams and spam at: www.nadicent.com/securitynewsandalerts.*