Let's forget about a Cyber Attack for Now

The following PCI regulated companies should have a big cyber worry besides ransomware and other cyber-attacks

Retail Stores

Restaurant

Tavern/ Bar

Jewelry Store

Auto Dealer

Furniture Store

Food Store

Doctor Office*

Dentist Office*

Hospital*

Pharmacies*

Clinic*

All these businesses are required to conform to PCI regulations. The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards. The **PCI** Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.
There are 4 levels of PCI compliance, Merchants processing:

I. Over 6M card transactions per year
II. 1-6M card transactions per year
III. 20,000 to 1M VISA eCommerce transactions per year
IV. Fewer than 20,000 on-line transactions a year or any merchant processing up to 1M regular transactions per year

* Please note that a number of companies have multiple regulations. All marked above besides PCI these companies also have HIPAA regulations.

The fines for non-compliance are significant! PCI non-compliance can result in penalties up to **$100,000 per month**. HIPAA fines can range from $100 to **$50,000 per violation**, with a maximum penalty of **$1.5M** per year for each violation.
The two must damaging penalties for companies not complying is losing your vendor contract and or your company is forced into bankruptcy & closing.

Other regulations

- **Cyber Insurance policy coverage** requires plans, policies, specific training of employees
- More vendor contracts now **require proof** of a cyber security program
- **Other- HIPAA, DFARS, FARS,** NY State, California, Gramm-Leach-Bliley, ENISA &GDPR (EU)

Cyber Attacks is only ½ the story!

Cyber fines from PCI, HIPAA or DFARS can and has put SMB companies out of business

SMBs make up 90% of the data breaches that impact businesses. Malicious hackers specifically target SMBs. More likely than not, it's because SMBs are more likely to have weaker security measures in place.

PCI is not, in itself, a law. The standard was created by the major card brands Visa, MasterCard, Discover, AMEX and JCB. At their acquirers'/service providers' discretion, **merchants that do not comply with PCI DSS may be subject to fines**, card replacement costs, costly forensic audits, brand damage, etc., should a breach event occur.

Let's say your retail business has suffered a data breach. First, the card brands will go to your acquiring bank (the bank that processes credit card transactions for you) and assess how well the bank has tracked your PCI compliance. Once they've ascertained the bank's level of monitoring and enforcement, they may fine the bank if you were not compliant at the time of the breach, and there will typically be penalties related to the breach as well. **And the bank will very likely pass on the fines and penalties to you.**

Powered by ACS

Ultimate **Risk** Services
SAVINGS THRU SAFETY & SECURITY

2874 W Ridge Pike | Norristown, PA 19403
610-755-0728 | www.ultimateriskservices.com