Ransomware is everywhere

The information presented below is a compilation of internet search results in mainstream media outlets to show prevalence of Ransomware and its impact to small medium business.

ABC7

http://abc7.com/search/?query=ransomware

LA Valley College paid $28K cyber-ransom to hackers

Monday, January 09, 2017

Los Angeles Valley College paid a cyber-ransom in order to get back online after the school's computer network came under attack, officials confirmed.

USA Today

http://www.usatoday.com/search/ransomware/

Search Ransomware and find 23 articles including one that talks about Ransomware as a service – explaining how criminals rent out their ransomware platforms to other criminals who don't have the technical expertise to build their own.

Inc Magazine

http://www.queryly.com/inc_advance.htm?searchkey=ransomware

search reveals 15+ articles about ransomware.

Entrepreneur Magazine

https://www.entrepreneur.com/article/286431

March 2, 2017- highlighted Ransomware in an article about how it is costing small businesses 75 Billion a year.

Forbes Magazine

https://www.forbes.com/search/?q=ransomware#23db0bea279f

Search reveals multiple articles about ransomware including one about how Ransomware has made its way onto primetime TV.

Prime Time Television

Ransomware was a plot in the season premiere of Mr. Robot and was featured in an episode of Homeland.

NBC News
http://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746
Reports on multiple small town police departments hit with ransomware. In January 2017 Police in Cockrell Hill, Texas reported that they lost 8 years' worth of evidence to ransomware. The department says the infection was discovered on December 12, last year, and the crooks asked for a $4,000 ransom fee to unlock the files. After consulting with the FBI's cyber-crime unit, the department decided to wipe their data server and reinstall everything. Data could not be recovered from backups, as the backup procedure kicked in shortly after the ransomware took root, and backed up copies of the encrypted files. The infection reportedly took place after an officer opened a spam message from a cloned (spoofed) email address imitating a department issued email address.

Tripwire – a security solution company published an article dedicated to January 2017 the month in Ransomware
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/january-2017-month-ransomware/
The year of 2017 isn't shaping up to be a game changer in combatting ransomware so far. On the contrary, crypto infections are becoming increasingly toxic in terms of their impact and attack surface. Online extortionists keep hitting police departments, healthcare organizations, public libraries, schools, hotels, and unprotected servers around the globe.

So how do you protect your business?

Preparation is the best way; to be prepared you need to have three things in place:

1. Employees that are aware and educated on data security practices
2. A Business Continuity Plan in the event of an attack
3. A back-up/recovery solution that is off-line and is tested for restorability

Your technology partner should be able to assist you with all three of these items. If you don't already have these in place, contact ITS, we can quickly get you set-up so you are confident your business is protected and prepared. If you would like us to set-up an in house test to see how vunerable your business is to this type of threat, just ask for the in-house demo when you call.

805-520-7020 or 800-876-4487

www.itstelecom.com/ransomprotection