APRIL 2019
ISSUE 4

Mobile Banking App is HERE!

UNION BANK

Ransomware:
Assessing the Business Risk

The statistics on ransomware remain alarming and show that it is still a growing threat. It has been reported that in 2019, a ransomware attack will be launched against a new organization every 14 seconds. Thus far, phishing emails have increased 109 percent from 2017. With all this distressing information about ransomware, many cybersecurity professionals don't believe that organizations are prepared for a ransomware attack.

Ransomware is a malware that locks data until the victim pays for its decryption. When data or software is inaccessible, it can slow business operations, cost a company money and damage its reputation. Sometimes, a business may feel the only option is to negotiate with cybercriminals and pay the ransom so the data can be released. But the outcome of a ransomware attack is not always cut and dry. Because of this, it's critical for businesses to address the growing threat of ransomware as a business risk as well as an IT concern.

When a ransomware attack occurs, time is critical. The longer an organization waits to respond, the longer its business functions and reputation could be in real jeopardy, so it's important that businesses create a response plan for a ransomware incident before an attack occurs.

While the response of each business will be different, there are several factors companies should consider before a threat occurs. Having a thought out process to deal with an incident before it occurs will not only assist in resolution but also show customers, stakeholders and the public that the enterprise has a well-reasoned strategy for dealing with ransomware incidents.

Below are some things to consider when assessing the risk to your organization.

Your Data is Important: Organizations should take inventory of their data and systems, identifying the operational critical pieces. Determining specific criteria before hand will make responding to a ransom request easier should an attack occur.

Inside This Issue

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

No Guarantees Many companies consider paying ransom when they have been attacked because in their assessment it might be the easiest way to release compromised data. But before a decision like that is made, it is important to know that there's never a guarantee that criminals will release the information. Companies need to have a strategic plan for dealing with the possibility their data may not be released and the impact it may have on daily business operations.

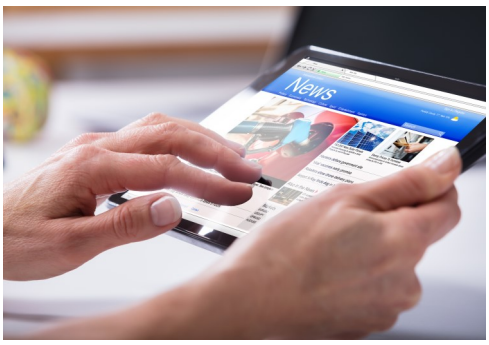
Content of Your Data –Understanding what data an organization possesses and where it is stored is crucial**.** This information is critical to determine how to deal with a ransom request. If a company has a solid backup of the data taken hostage, that may play into the decision making on how to deal with the cybercriminal.

Your Reputation –A company's reputation is everything, especially in this era of social media. It's never good when criminals take an organization's data hostage, but it can be particularly bad for organizations such as those in the financial, healthcare and educational sectors because these types of industries normally have large amounts of customer personal data. In addition to the importance of compromised data, enterprises should consider how their response to a ransomware attack will affect their reputation with customers, partners and shareholders.

There is no easy solution in a ransomware attack. It's important for organizations to think through possible ransomware attack scenarios ***before*** an incident rather than during . Having a clear and quick response plan will help deal with an attack and provide the best possible outcome for your company.

Sources:
https://phoenixnap.com/blog/ransomware-statistics-facts
https://www.securityweek.com/ransomware-four-ways-assess-growing-threat-business-risk

Using Your New Tablet Safely!



In the market for a new tablet? Well Apple just unveiled their new iPad and we know many are already in line to make that purchase. But whatever type of tablet you decide to purchase, it will most likely become an important extension of your life, even perhaps replacing your computer.

Here are some key steps you should take to keep your tablet and your information safe and secure.

- First things first, enable automatic locking of the screen so every time you want to use your tablet, you first have to unlock the screen with a strong passcode, swiping pattern or your fingerprint.
- Track your device. Install or enable software to remotely track your new tablet over the Internet. This way, if your tablet is lost or stolen you can potentially connect to it over the Internet and find its location.
- When configuring your tablet for the first time, make sure to check the privacy options. Also, check the privacy settings and permissions on any app downloaded.
- Only download apps you need and those from trusted sources.
- Update your device and enable automatic updating. Just like a computer, app developers are constantly sending patches to fix vulnerabilities and bugs.
- Disable the sharing of any information feature. Don't allow your private information to be accessible through the cloud.

Your tablet is a powerful tool, one that we want you to enjoy and use. Just remembering these few simple steps can go a long way to keeping you and your new tablet safe and secure.

Sources
https://usa.kaspersky.com/resource-center/preemptive-safety/tablet-security-safety