



Computer breach exposes Timken employee files

Reposity staff water
CANTON Personal information or
CANTON Personal information or
mer employees – as well as applicant
materials of the control of the control of the control
materials of the control of the control
became accessable online. occ unasable
trial occess to the data file, but no evi
dence of fraudulent use of the information, the company said in a statement
to, the company said in a statement
Timben said it discovered the insidere
File. 13 and removed the file from the
company's server. The file — mistakees
y invend to a server used to enchange
y mored to a server used to enchange

receive anected yet network new to retired via a leaver. Timbers steps to protect the step of the step

people in 32 states, according to the letter. The file contained names, Social Security numbers, birth date and gender, saw that as realist from the person's employment hearing screening.

Thinkes not it has a team working with law employment the same than the same th

Ohio Physicians Clinic Shuts Down After Ransomware Attack

January 25, 2016

Ransomware Leaves Ohio Clinic Inoperable

We've heart of ransomware infections infecting hospitals and clinics. We've also heard that at times patients have been sent away because some of the more sophisticated procedures could not be done. Now, a medical clinic in northeastern Ohio has been completely shut down due to a ransomware attack. Pulmorany Physicians is now on its fifth day without critical files, making it impossible to see patients. The facility was desping all of their files stored on services in the cloud through Allscripts. Last week, Allscripts was hit with a ransomware attack. It was this attack that led

to the encryption of Pulmonary Physicians; data. At this sime, it remains unknown how long it will take to unlock the files. Understandably, all impacted facilities want this resolved as soon as possible. However, to the only way to get business operational again, after a ransomwaie reflection is to restore using backup felse. This can be incredibly time consuming. So, time consuming in fact, a hospital in Indiana recently paid the \$\$5,000 ransom demand, even when they had backup files because it was more cost effective to pay the demands and gain almost immediate access to their files again. Although, P.C Masic does not encourage ransomwaie vectimes pay the ransom demands. By doing so, a target goes on the facility for future ransomwaie vectime pay the ransom demands. By doing so, a target goes on the facility for future ransomwaie vectime attacks. There is also no guarantee that paying the ransom demands will unlock the file.

Pulmonary Physicians Inc 2600 Tuscarawas St W# 100, Canton, OH 44708

Email hackers scam \$1.7M from Boardman business

Posted: Jan 26, 2018 12:57 PM EST Updated: Feb 01, 2018 8:48 PM EST

By Cristen Manion, Multi Media Producer CONNECT



BOARDMAN TWP., Ohio - A Boardman business discovered more than \$1,750,000 missing from their bank accounts.

Boardman police say the Federal Bureau of Investigation has been called after someone was able to hack into a business email account for Boardman Molded Products.

According to the report, Daniel Kessler called police after learning about the missing money.

(A) Huntington

2

Top 5 Reasons For Cyber Insurance

- 1. Malicious/criminal attack, human error, and system glitches
- 2. Retaining physical or electronic records
- 3. 95% of businesses rely on their computers systems to operate
- 4. Ransomware is evolving. Infections were up 40% last year.
- 5. 49% of organizations with at least one significant attack were successfully attacked again within one year.

(A) Huntington

3

Cyber Liability Insurance

A cyber liability policy provides 1st and 3rd party coverage for damages when private, personal, or financial information is compromised due to a data breach or network intrusion. While exact wording and terms may vary, our goal is to match the right coverage for the exact exposures of the insured.

Huntington



Cyber is evolving

\mu Huntington 📗

6

Traditional and Evolving Exposures

- Credit Card Processing
- Sensitive Data Storage
- Lost or Stolen Devices
- Improper disposal or information access
- Malicious or Accidental Employee Actions
- Virus transmission
- Phishing Attacks
- Business Email Compromise
- · Vendor Activities
- Ransomware
- Online Payment Activity

(#) Huntington

7

Social Engineering

Coverage for loss of money or securities due to a person impersonating another and fraudulently providing instructions to transfer funds.

- > Not covered under most standard policies without endorsement
- > The key to this coverage is that the attack is by trick or scheme

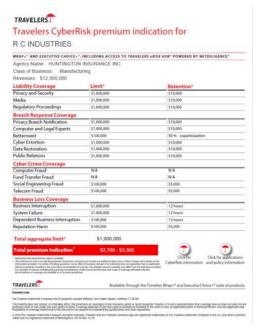
Huntington



Best Practices

- Full audit of cyber coverage
- Make sure there are proper protocols and procedures in place
- Get training
- Monitor the cyber program

(#) Huntington



Huntington

11



