



1



Ohio Physicians Clinic Shuts Down After Ransomware Attack

January 25, 2018

Ransomware Leaves Ohio Clinic Inoperable

We've heard 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. Pulmonary Physicians is now on its fifth day without critical files, making it impossible to see patients. The facility was keeping all of their files stored on servers 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 time, 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 ransomware infection is to restore using backup files. This can be incredibly time consuming. So, time consuming in fact, a hospital in Indiana recently paid the \$55,000 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, PC Matic does not encourage ransomware victims pay the ransom demands. By doing so, a target goes on the facility for future ransomware attacks. There is also no guarantee that paying the ransom demands will unlock the files.

Pulmonary Physicians Inc.
2800 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.

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.

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.



5

Cyber is evolving

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

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



9

Best Practices

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

TRAVELERS
Travelers CyberRisk premium indication for
R C INDUSTRIES

WRAP+[®] AND EXECUTIVE CHOICE+[®], INCLUDING ACCESS TO TRAVELERS #RISK HUB[®] POWERED BY NETDILIGENCE[®]

Agency Name: HUNTINGTON INSURANCE INC
 Class of Business: Manufacturing
 Revenues: \$12,900,000

Liability Coverage	Limit*	Retention*
Privacy and Security	\$1,000,000	\$10,000
Media	\$1,000,000	\$10,000
Regulatory Proceedings	\$1,000,000	\$10,000
Breach Response Coverage		
Privacy Breach Notification	\$1,000,000	\$10,000
Computer and Legal Experts	\$1,000,000	\$10,000
Betterment	\$100,000	50% coparticipation
Cyber Extortion	\$1,000,000	\$10,000
Data Restoration	\$1,000,000	\$10,000
Public Relations	\$1,000,000	\$10,000
Cyber Crime Coverage		
Computer Fraud	N/A	N/A
Fund Transfer Fraud	N/A	N/A
Social Engineering Fraud	\$100,000	\$5,000
Telecom Fraud	\$100,000	\$5,000
Business Loss Coverage		
Business Interruption	\$1,000,000	12 hours
System Failure	\$1,000,000	12 hours
Dependent Business Interruption	\$100,000	12 hours
Reputation Harm	\$100,000	\$5,000

Total aggregate limit* \$1,000,000
Total premium indication† \$2,700 - \$3,300

* Excludes first and second-occurrence retentions.
 † This indication is only a non-binding estimate of premium, and does not include any additional fees, fees or other charges and is based on the information provided. It includes a loading for expenses, such as after-the-fact coverage. Amount of the indication does not guarantee that an application will be accepted by Travelers. The actual premium amount will be provided by the underwriter upon completion of the underwriting process. The actual premium amount may vary due to the actual risk characteristics of the insured and the type and scope of coverage ultimately selected. Not all policies or coverages are available in all states.

TRAVELERS Available through the Travelers Wrap+[®] and Executive Choice+[®] suite of products.

© 2018 The Travelers Indemnity Company. All rights reserved. Travelers and the Travelers emblem logo are registered trademarks of The Travelers Indemnity Company in the U.S. and other countries. #Risk Hub is a registered trademark of NetDiligence. 18114 Rev. 12/18



Q&A

