

Ransomware - Is Your Insured's Firm Vulnerable?

It is one of your clients worst nightmares. They turn on the computer and there is a ransom note on the screen. Whether they are in the office or working from home, the attacker has used their computer to gain access to the firm's entire network resulting in a complete lockdown. What should be done? Ideally the employer's incident response plan will guide their next steps which should include immediately contacting their cyber carrier for guidance.

But what is Ransomware? This is a malicious type of software (malware) that attempts to extort money from victims by denying access to a computer system or files. The most prevalent form of this malware, crypto-ransomware, encrypts files that can only be decrypted with a key held by the malicious actor.

Some malware is designed to harvest personal and proprietary information before initiating the ransomware. Once successful at infiltrating your system, personal data, passwords, mail files, browser data and more are all at risk. This is just a stepping stone, giving your attacker access to even more sensitive data such as personal / business bank accounts and client information including personal identifiable information (PII).

A new twist to this scheme is where cybercriminals are not just encrypting data but stealing it and threatening to release it on the internet. These new extortion attempts are no longer only about getting data back but also about the risk of proprietary data being exposed or sold to third party. Whatever the situation, ransomware can have severe business consequences!



If your client's firm is hit with ransomware:

DO:

- Consult their incident response plan
- Contact you as their broker so that the Insurer can be put on notice
- Preserve all electronic artifacts

DON'T:

- Shut down or reboot infected systems
- Communicate with the threat actor by yourself or have the local IT provider call the threat actor
- Wipe out anything on your network

Call Russell Bond today to learn how together we can help protect your clients and their livelihoods. We have access to many markets offering several products, covering a variety of Cyber crimes no one ever wants to experience!

Call us for more information: 800-333-7226



Tonya Hollederer, ext. 133
Product Lead
thollederer@RussellBond.com



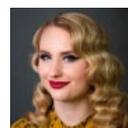
Ed Chadwick, ext. 261
echadwick@RussellBond.com



Jackie Oddo, ext. 161
joddo@RussellBond.com



Malissa Smith, ext. 148
msmith@RussellBond.com



Natalie Golubski, ext. 132
ngolubski@RussellBond.com

A Wholesale Insurance Broker Unlike Any Other™