Courtesy of
The Insurance Exchange

# CYBERRISKS&LIABILITIES_

## Ransomware

The damage caused by global ransomware is predicted to exceed $5 billion in 2017, according to researcher Cybersecurity Ventures. Up from $325 million in 2015, the costs represent not just the amount of the ransom, but also the costs of downtime and lost productivity.

Ransomware is any type of malicious software that infects a computer and either prevents it from working as it should or prevents access to certain files until the user pays a ransom. Typically, the hackers behind the ransomware demand bitcoin—a type of digital currency that is difficult for police to trace.

Businesses of all sizes have become targets of ransomware, as it can infect not only personal computers, but also entire networks and servers.

**How Ransomware Can Spread**
There are different ways that ransomware can spread, including the following:

- Visiting fake or unsafe websites
- Opening emails or email attachments from unknown sources
- Clicking on suspicious links in emails or on social media

**What Ransomware Does to Your Computer**
There are two main types of ransomware that can hold computer systems hostage:

- Lock-screen ransomware works by displaying a window on the computer's lock screen that attempts to prevent access to the computer. The message on the lock screen may even claim to come from the federal government, accusing the user of violating a law and demanding a fine.
- Encryption ransomware works by keeping the computer available but encrypting certain types of files, thus making them unreadable. The files most commonly affected are those that include sensitive information and are assumed by the hacker to be of the most value. When people try to access the files, they then see a pop-up screen that instructs them to buy a private decryption key that can decrypt the scrambled files.

**How to Respond**
Some operating systems provide instructions for responding to lock-screen ransomware, although results aren't guaranteed. In contrast, encryption ransomware has no quick fix without an encryption key, which only the hackers typically have access to.

Regardless of the type of ransomware, experts recommend against paying the ransom. After all, there is no guarantee that you will regain access to your computer, network or files after you pay. Furthermore, by paying the ransom, you could be encouraging future cyber crimes.

If your business is affected by ransomware, take the following steps:

- Report the event to your local FBI office.
- File a complaint with the Internet Crime Complaint Center.
- Restore file backups, if you have them.
- Check your insurance coverage to see if it covers the costs of ransom money paid and lost business.

**What to Do if You've Already Paid the Ransom**
Since business can come to a halt without access to essential data, business owners are often tempted to pay the ransom in order to quickly regain access. If

THE INSURANCE EXCHANGE
Since 1967
www.TIE-inc.com

you've paid the ransom, contact your bank and call the police as soon as possible. Credit card companies may be able to block the transaction and refund you if you contact them promptly.

The Federal Trade Commission's OnGuard Online website is a good resource for more tips on what to do if you're affected by ransomware or any other type of internet fraud.

**How to Protect Your Business**

Cyber extortion from ransomware is a legitimate threat to all businesses—no matter the size. The best method of prevention is to keep confidential information and important files securely backed up in a remote location that is not connected to your main network.

In addition to backing up your files, taking the following prevention measures can help keep your information secure and prevent you from becoming a victim of cyber attacks:

- Teach your employees about ransomware and the importance of preventing it.
- Show your employees how to detect suspicious emails and attachments. For example, watch for bad spelling or unusual symbols in email addresses.
- Develop a protocol for reporting incidents of ransomware and other suspicious cyber activity.
- Develop a schedule for regularly backing up sensitive business files.
- Update your company software as soon as new updates are released. In doing so, you can patch the security vulnerabilities that cyber criminals rely on, and avoid becoming an easy target.
- Purchase cyber liability insurance that not only helps you respond to threats, but can also help cover the cost of the ransom and any other losses incurred as a result of cyber extortion.

Don't let ransomware—or any type of cyber exposure—threaten your business. Contact The Insurance Exchange to ensure you have the proper coverage and the tools necessary to protect against losses from cyber attacks.