Imagine walking into your office, turning on your computer, and seeing nothing but a message demanding bitcoins in return for unlocking all your company’s files. The nightmare known as ‘Ransomware’ recently became all too real for more than 200,000 computers in more than 150 countries, bringing some hospitals and other organizations to a halt. While those affected were primarily outside the U.S., experts say the perpetrators are ramping up their efforts and they warn all businesses to take steps to prepare.

The information typically available within the workers’ compensation system — social security numbers, personal health information, etc., — makes it a must for the industry to take notice of the situation. The good news is there are ways to shield and prevent such attacks from infiltrating your company.

What Is Ransomware

Ransomware takes the idea of hacking to a whole new level. Those spearheading the efforts are not necessarily interested in stealing your data, they really just want to hold it hostage until you pay up — hence the term.

Businesses large and small may be equally at risk. In fact, small businesses may be even more at risk than larger ones because of their often more relaxed attitude about cyber security.
Ransomware is sophisticated malware that blocks access to a computer by encrypting the data or system until it is unlocked. ‘WannaCry,’ the malware used in the recent incident, is not the only ransomware out there and, in fact, there are even copycat versions of WannaCry now available on the black market.

The wrongdoers look for the easiest way to infect a system or network and use it as a means to spread the malicious content. Often, it is through an unwitting employee. Phishing is one of the main ways of accessing a computer, where someone sends emails that that appear to be from legit companies, but are not.

Another method is for someone to send a fraudulent email that appears to come from a high-ranking company official seeking sensitive information or money transfers. Lost devices, such as laptops, phones and physical files are another way to break in to a company’s network.

**Ransomware Preventive Measures**

- **Back it up - twice.** An external hard drive should be used for backing up all your files and data; then it should be disconnected from the computer. The cloud may be used for a second backup, such as Dropbox, Google Drive, or OneDrive. However, the cloud application should not be turned on except once per day to sync the data. Another backup source can be an ‘air gapped’ computer or server, that is secure and isolated from other networks.

- **Train employees.** Unfortunately, unwitting employees may be the most vulnerable part of your cyber security. It’s imperative they understand and are kept up to date on what and how cyber-attacks and ransomware occur and how to prevent them. You can then periodically test employees with mock phishing emails. The training should be ongoing and should include the following:

  - Review emails closely to make sure they are from a trusted and known sender before links or attachments are opened.
  
  - Never download attachments from spam or suspicious emails.
- Bring Your Own Device (BYOD) training to highlight the risks in downloading suspicious apps on them. On smartphones, only official materials should be downloaded.

- Don’t store important data on the PC, if possible.

**Update software.** Computers and software that are outdated are more likely to crash and face cyberattacks. Security updates for Microsoft and other operating systems should be applied immediately, including any patches released to combat WannaCry or malware. Antivirus and anti-spam filters should also be kept current.

**Implement/update security policies.** Passwords should be strong; meaning they should contain upper and lowercase letters as well as numbers and symbols; and they should be changed at least every 90 days. A companywide password policy should be strictly enforced. Computer browsers’ security and privacy settings should be adjusted for better protection. Outdated plugins and add-ons should be removed from the browser. An ad blocker should be used to prevent potentially malicious ads.

**Check your policy.** If your company does not have a cyber policy, explore the idea of getting one. These typically cover the cost of notifying those whose data has been affected, and even hiring a public relations firm to combat reputational damage. If you have a policy it’s vital to inform the insurer if and when a breach occurs. Other policies that may include coverage are kidnap and ransom, or property policies. In the event of a breach these may help pay for legal costs, data restoration, business interruption and the ransom, if paid.

**Incident response plan.** Your company should consider forming an action plan that would kick into effect in the event of a security breach, to help limit costs and damages. It should guide personnel at all levels to help manage the breach. Once implemented, you can run simulated attacks to test your company’s level of preparedness.
Author Michael Stack, Principal, Amaxx LLC. He is an expert in workers compensation cost containment systems and helps employers reduce their work comp costs by 20% to 50%. He works as a consultant to large and mid-market clients, is co-author of Your Ultimate Guide To Mastering Workers Comp Costs, a comprehensive step-by-step manual of cost containment strategies based on hands-on field experience, and is founder & lead trainer of Amaxx Workers’ Comp Training Center.

Contact: mstack@reduceyourworkerscomp.com.

Workers’ Comp Roundup Blog: http://blog.reduceyourworkerscomp.com/

©2017 Amaxx LLC. All rights reserved under International Copyright Law.

Do not use this information without independent verification. All state laws vary. You should consult with your insurance broker, attorney, or qualified professional.

This entry was posted on Monday, May 22nd, 2017 at 5:10 pm and is filed under Risk Management
You can follow any responses to this entry through the Comments (RSS) feed. You can skip to the end and leave a response. Pinging is currently not allowed.

This PDF document can’t be printed.

Unnecessary printing not only means unnecessary cost of paper and inks, but also avoidable environmental impact on producing and shipping these supplies. Reducing printing can make a small but a significant impact.
Powered by Unprintable Web for WordPress - www.greencomputingportal.de