CYBERRISKS+LIABILITIES

IN THIS ISSUE

JRG ADVISORS

Educate Your Employees During National Cyber Security Awareness Month

This October is Cyber Security Awareness Month, an event co-sponsored by the Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA) in order to raise awareness of the importance of cyber security issues. While the event is designed to highlight some of the nation's cyber security precautions, as well as how to be prepared in the event of a national cyber security incident, much of the focus is on good cyber security practices for the average individual.

Specifically, the groups are trying to promote their "Stop. Think. Connect." and Stay Safe Online campaigns—efforts that teach good cyber security in terms everyone can understand. In order to encourage your employees to practice good cyber security, review the following lessons with them:

- **Password Security:** More powerful computers have given criminals the ability to crack passwords easily. Passwords with a mix of capitalized and lowercase letters—as well as numbers, symbols and other special characters—are much harder to crack. And, though it should go without saying, make sure your employees don't write their passwords down in plain sight in their work spaces.

- **Phishing Scams:** A number of different scams could fall into this category, but they all have commonalities that your employees should be aware of. Never open an email from an unknown source, and never click on a link in an email unless both the sender and the link can be trusted.

- **Software Updates:** Security patches are designed to fix known vulnerabilities. Make sure your employees download the latest security patches when they become available.

Those wishing to participate in this year's activities can find a number of resources available online, or contact your partners at JRG Advisors, LLC for further cyber security materials.

68 Million Users Affected by Dropbox Data Breach

Journalists at Motherboard reported that they obtained documents which show that more than 68 million users were affected by the data breach at Dropbox—one of the world's largest file-hosting companies.

The information contained in the documents has since been identified as authentic by officials at Dropbox, though the company wanted to reiterate that this information didn't refer to a new data breach. Rather, the documents detailing usernames and passwords stemmed from a 2012 data breach, an incident which had already been known.

So, while this isn't a new breach, and while those affected by the breach in 2012 had already been told to change their passwords, those who reused the same email and password combination at other sites might now be vulnerable.

Global Cyber Crime to Top $6 Trillion by 2021

According to a new Cybersecurity Ventures report, the global cost of cyber crime will double in the next five years, exceeding $6 trillion annually by 2021. That figure includes a number of costs, including those stemming from the value of the data itself, restoration costs, lawsuits, stolen money, fraud and a host of other related expenses.

There are a number of factors to blame for the increase, including the rise of state-sponsored cyber crime. However, the sheer volume of data could have the biggest impact. According to some estimates, the increased digitization of records and the promulgation of the Internet of Things mean that, by 2020, the globe will have 50 times more data to protect than it does currently.

The report also predicts that cyber crime will begin to grow in new sectors. For instance, construction—an industry that has been a late adopter of many technological innovations—is an industry that many experts predict will see a rise in cyber crime. As it does, device manufacturers, contractors and workers themselves will have to become more diligent about cyber risks, and businesses will have to consider emerging cyber exposures.

Ransomware Attack on NASCAR Crew Leads to New Sponsor

After a ransomware attack locked a NASCAR crew chief out of his computer, Circle Sport-Leavine Family Racing (CSLFR) will be changing its primary sponsor to Malwarebytes—the company responsible for helping the team in the aftermath of the attack.

In April, as the team was preparing for a Sprint Cup race, CSLFR crew chief Dave Winston discovered that a number of files on his computer had been encrypted. Those files included documents and spreadsheets containing data on the team's car. According to CSLFR, that data represented thousands of hours of work and was worth over $1 million.

The hackers that installed the ransomware also included a note, demanding $500 in bitcoins for a key that would unlock the files. After learning that the data was probably lost without that key, CSLFR found a bitcoin ATM, paid the ransom and received the key the following morning.

At present, no one knows precisely how the computer first became infected, but the team wanted to make sure it wasn't struck again. That's when it first reached out to Malwarebytes for advice and tools to help protect the team's systems from malware. Quickly, that partnership evolved, and the parties came to a sponsorship arrangement.

Winston, the rest of his team and their partners at Malwarebytes expressed hope that sharing their story would help raise awareness about the problem of ransomware. They also hope that advertising a company like Malwarebytes on the number 95 car will encourage NASCAR fans to be proactive about cyber security.

For more information on ransomware, or other cyber security resources, contact your partner at JRG Advisors, LLC today.

.

JRG Advisors, LLC
7000 Stonewood Drive, Suite 251
Wexford, PA 15090
412-456-7000
http://www.jrgadvisors.net/