BROWNEDWARDS
certified public accountants

InfoSec Update

August 11, 2015

"There are only two types of companies: those that have been hacked, and those that will be."

~ Robert Mueller, FBI Director, 2012

In this edition of InfoSec Update we will cover a few major issues in the world of Cybersecurity.

First up are some articles that impact everyone who deals with sensitive and private data. On Monday July 21st the U.S. Court of Appeals for the Seventh Circuit issued a ruling that may make it easier for customers to take organizations to court over data breaches. Previously customers had a hard time taking their claims to court due to a ruling called the "Clapper" case. This case required consumers to show a "risk of imminent and concrete injury", and has frequently been sighted in the past to prevent class action lawsuits against organizations that have suffered a data breach. In 2013 Neiman Marcus suffered a data breach and as a result credit card data for 350,000 customers was exposed. Of those accounts exposed Neiman Marcus agreed that 9200 of the accounts were later used in fraudulent activity. Customers affected by the breach later filed a class action suit seeking "at least five million in damages". The company argued that the customers did not suffer damage as they were later reimbursed by the card companies for the fraudulent activity. The customers countered that time and money spent to correct the issue was not taken into consideration nor was the threat of future damage from the breach. The case was initially dismissed, but on July 21st the Seventh District court overturned this ruling. The overturned ruling reinstated both types of claims, the loss incurred due to the breach and those that feared loss due to possible fraudulent activity in the future. Chief Judge Diane Wood said that fear of hackers in the future is not to "speculative" for legal action. Wood also wrote "Why else (other than to cause harm) would hackers break into a store's database and steal consumer's private information?"

The Seventh Court of Appeals is one of the nation's most influential appeals court and has a reputation for being business friendly. This is particularly bad for businesses that are facing class action suits for data breaches. Companies going forward will have to defend themselves in court when in the past these cases would have simply been dismissed.

This brings up many questions about liability. How much protection is enough? Do I have the right controls in place to prevent these types of issues? Will "cyber" insurance cover these types of incidents? Will insurance premiums rise as a result? What information will insurers look to prior to covering an organization? Stay tuned to the Brown Edwards InfoSec Newsletter for updates and information about this complex and rapidly growing topic.

Articles used for this update;

http://blogs.wsj.com/cio/2015/07/23/appeals-court-revives-neiman-marcus-data-breach-suit/
http://fortune.com/2015/07/29/data-breach-7th-circuit/

TECH FACTS IN THE NEWS

Many of you have heard of the recent hacking of a car to make it do a variety of things even stopping the vehicle while it was in motion. One of the reasons that this is important is the "Internet of Things" (IoT) which is defined as the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable objects to exchange data with the manufacturer, operator and/or other connected devices. Below are some links to some articles that illustrate how these "things" can be hacked and used for malicious purposes.

The original article of the Jeep which was hacked:
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Hacking of electric skateboards that can cause injury:
http://www.wired.com/2015/08/hackers-can-seize-control-of-electric-skateboards-and-toss-riders-boosted-revo/

Hacking of a "smart" sniper rifle to disable the rifle or even change its target:
http://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/

A gadget that can be used to locate, unlock and start GM cars:
http://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/

As most of the readers of this newsletter are Windows shops I have included a review of Windows 10 by ArsTechnica:
http://arstechnica.com/gadgets/2015/07/review-windows-10-is-the-best-version-yet-once-the-bugs-get-fixed/

Last is an article from DarkReading about the increase of attacks using the RIG 3.0 Crimeware Kit:
http://www.darkreading.com/attacks-breaches/web-attacks-employing-upgraded-crimeware-kit-hit-15-million-users-/d/d-id/1321580?

Please contact us to discuss any of the articles or any item or interest or concern, Call 540 434-6736 or email BrownEdwards@becpas.com

To opt out of future emails please reply with STOP in subject line.

Disclaimer: This information is offered for informational purposes only and should not be taken as legal advice.

BROWNEDWARDS
certified public accountants