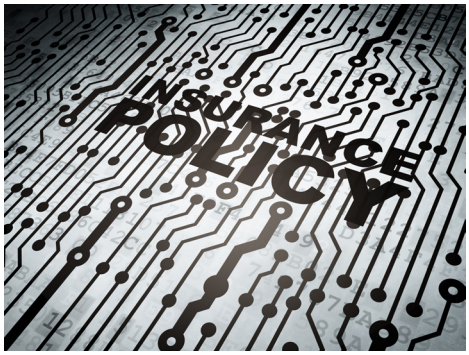
Business System Solutions
July 2017

The BSS Advisor



The Dirty Loophole That Lets Insurance Companies Refuse to Cover a Cybercrime Theft in Your

As hacking hit the headlines in the last few years — most recently the global hack in May that targeted companies both large and small — insurance policies to protect businesses against damage and lawsuits have become a very lucrative business indeed. Your company may already have cyber insurance, and that's a good thing. But that doesn't mean that you don't have a job to do — or that the insurance will cover you no matter what.

When you buy a car, you get the warranty. But in order to keep that warranty valid, you have to perform regular maintenance at regularly scheduled times. If you neglect the car, and something fails, the warranty won't cover it. You didn't do your job, and the warranty only covers cars that have been taken care of.

Cyber insurance works the same way. If your company's IT team isn't keeping systems patched and up to date, taking active measures to prevent ransomware and other cybercrime attacks, and backing everything up in duplicate, it's a lot like neglecting to maintain that car. And when something bad happens, like a cyber-attack, the cyber insurance policy won't be able to help you, just as a warranty policy won't cover a neglected car.

"If your company's IT team isn't keeping systems patched and up to date, taking active measures to prevent ransomware and other cybercrime attacks, and backing everything up in duplicate, it's a lot like neglecting to maintain that car."

Check out this real life policy exclusion we recently uncovered, which doesn't cover damages "arising out of or resulting from the failure to, within a reasonable period of time, install customary software product updates and releases, or apply customary security-related software patches, to computers and other components of computer systems." If your cyber insurance policy has a clause like that — and we guarantee that it does — then you're only going to be able to collect if you take reasonable steps to prevent the crime in the first place.

That doesn't just mean you will have to pay a ransom out of pocket, by the way. If your security breach leaves client and partner data vulnerable, you could be sued for failing to protect that data. When your cyber insurance policy is voided because of IT security negligence, you won't be covered against legal damages, either. This is not the kind of position you want to be in.
All of this is not to say that you shouldn't have cyber insurance, or that it's not going to pay out in the case of an unfortunate cyber event. It's just a reminder that your job doesn't end when you sign that insurance policy. You still have to make a reasonable effort to keep your systems secure — an effort you should be making anyway.

Lafayette Office:
1211 Cumberland Ave.
West Lafayette, IN 47906
(765) 742-3440

Kokomo Office:
3138 S Lafountain St.
Kokomo, IN 46902
(765) 507-9583

www.bssconsulting.com

BSS is your IT Partner providing **Total Care** support for all your technology needs with exceptional **Customer Service** and the best IT Solutions to make ***your business*** more productive and profitable!

IT Security Tip #18: Your firewall is USELESS unless...

A firewall is a device that acts like a security cop watching over your computer network to detect unauthorized access and activity – and EVERY business and individual needs one.

However, your firewall is completely useless if it's not set up or maintained properly. Your firewall needs to be upgraded and patched on a continual and consistent basis, and security policies and configurations set. This is not something you want to try and handle on your own – you are best served by letting the pros (us!) handle that for you.

If you're a BSS client, we've got you covered. If not, give us a call at (765) 742-3440.

Time To Upgrade - Majority of Wannacry Victims Were Running Windows 7

The recent "Wannacry" hacking attack was global in its scale, impacting companies in more than 150 nations before it was stopped by a security expert with a good eye. It was such a dangerous, widespread attack that Microsoft even took the highly unusual step of issuing an emergency patch for Windows XP users, even though they officially killed support for that platform some time ago.

Now that the dust has settled and security experts have had more time to analyze the dimensions of the attack, a startling new detail has emerged.

Overwhelmingly, the people who fell victim to the attack were running Windows 7. In fact, according to data released by Kaspersky Labs, more than 98 percent of impacted users were running that OS.

Like Windows XP, support for Windows 7 has formally ended, and although a quick-thinking researcher was able to stop the initial attack in its tracks by remotely accessing the malware's kill switch, you can bet that the hackers who launched the attack are taking steps to eliminate that possibility. Once they do, another global assault is all but assured, and next time, there may be no way of stopping it at all. In fact, security researchers have already found beta versions of Wannacry in the wild that have no kill switch, period.

If you haven't yet gotten around to migrating your old Windows 7 systems to something more robust and up-to-date, now is the time and the clock is ticking. **Call us today at (765) 742-3440 if you need to create a plan to upgrade your systems to keep them secure.**

The hackers aren't going to wait, and if you delay much beyond the point of reading these words, your company could be caught up in the next attack. This could mean having all the files on the infected computer encrypted, forcing you to either restore from the most recent backup you have, or pay the ransom and hope the hackers play fair and give you the unlock key. This is not a happy situation to find yourself in.

DID YOU KNOW?

- The term "genuine leather" isn't reassuring you that the item is made of real leather, it is an actual distinct grade of leather and is the second worst type of leather there is.
- Spacesuits take 5,000 man-hours to make and cost around $2 million.
- Saudi Arabia imports both sand and camels from Australia.
- Dr. Seuss created the word "nerd". Its first documented use was in the 1950 book If I Ran the Zoo.
- Killer bees are a manmade hybrid species that are only found in the wild because they accidentally escaped quarantine in 1957.
- When you get a sunburn, it's not your skin cells being damaged by the sun and dying, it's your skin cells' DNA being damaged by the sun and them killing themselves so they don't turn into cancer.
- In 2013 it cost $289,500 a year for a permit to run a hot dog cart near the Central Park Zoo.
- Despite having a wingspan of up to 7.5 feet and a height of up to 3.5 feet, a typical male bald eagle weighs only 9 pounds.
- Before 2012, the largest buyer of kale in the US was Pizza Hut, and it was only used as garnish around their salad bar.

ELECTRONIC WASTE RECYCLING DRIVE

8am-5pm Thursday, July 20 through Friday, July 21 we will be holding our Second Annual Electronic Waste Recycling Drive in West Lafayette.

We are accepting all electronic devices free of charge aside from CRT Monitors (the old big monitors) and Televisions which have a $10 fee per item.

We will also provide free data destruction for any hard drives or materials that may contain sensitive data. Just stop in and let us know!

"Here's what you're going to do. You're going to give those 3 million people their credit card numbers back and you're going to say you're sorry."

Chrome Discovery Gives More Reason To Cover Your Laptop Camera

An AOL developer named Ran Bar-Zik has unearthed a disturbing flaw in Chrome that may make you rethink using Google's web browser.

The issue revolves around a website's ability to activate your camera and audio recorder. Google uses an API which legitimate developers call, that displays a distinctive red dot on the browser tab when the page in question activates your laptop's camera and recording equipment (like it does when you activate a video call via a Google Hangout page, for example).

The problem is that this API is not required to be used, and an enterprising hacker can use malicious JavaScript to activate your camera without notifying you, and without any visible indication that the camera is on.

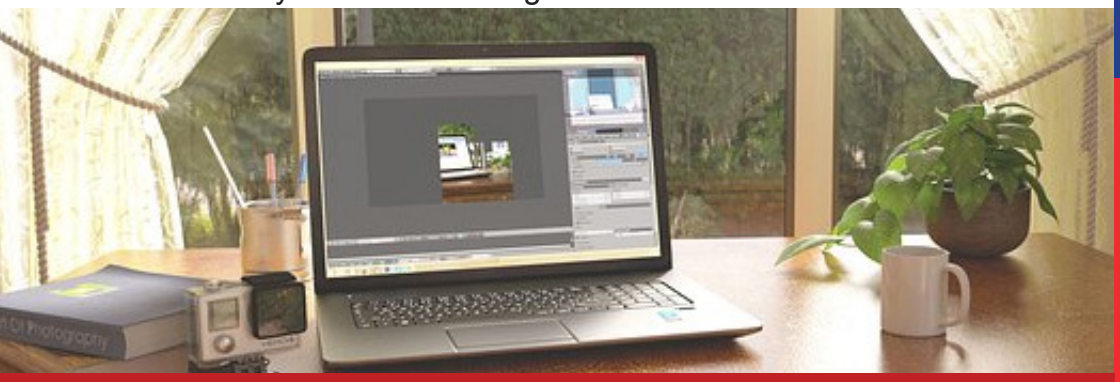
From a practical standpoint, that means that any webmaster using the code could spy on you, and you'd be none the wiser. Worse, although Google has been informed of this flaw, they've decided that it's not a critical security issue, so there are no immediate plans to issue a patch to correct it.

As a user, you don't really have many good options here, except to disable your equipment or cover the camera when you're not actively using it.

Neither of these are perfect options. If a hacker can remote-activate the camera, then they can also enable it, even if you've disabled it electronically or covered your camera lens. These measures also don't prevent a hacker from listening in on you and everyone in the immediate vicinity of your laptop.

These kinds of dangers are becoming increasingly common. Just last year, Samsung got into hot water over the fact that its Smart TV's record everything said in their vicinity, and that data is saved on a Samsung server where it could potentially be captured by hackers, and Amazon's Echo has made the news for similar reasons.

There are no easy answers or fixes here, so users beware.



Last month's question was: **Which late night host was born in Indianapolis? The correct answer was B) David Letterman. He was born on April 12, 1947.**

Jamie Bluera was drawn as the winner. Congratulations!

TECH TALK

You've Been HACKED! What's the First Thing You Should Do?

There's always a chance that IT security will be breached, and one way to make a bad situation worse is not knowing the standard operating procedure when it happens. First, contact your IT personnel. The faster they can address the hack and figure out its extent, the better served you'll be. Next, understand that there are legal ramifications to being hacked; if valuable data has been compromised, you'll have to notify the individuals in question as well as the FBI. Remember, the faster you act, the better it will be.

Alexa, Who's Winning the Virtual Assistant War?

There are multiple companies trying to break into the "smart home hub" market, but Amazon's Echo (and its sultry Alexa) are holding on to 70 percent of the market share, and it doesn't look like that's changing any time soon. That's a clear sign of victory for Amazon ¬- and a wake-up call for its competitors.

The voice-activated home assistant market is growing, with almost a third of millennials likely to use a home assistant this year. While it might take a decade or more for the devices to find their way into the homes of older demographics (a situation Saturday Night Live has already mined for comedy), it seems that smart hubs will only increase in popularity from here on out, and that Alexa is poised to rule them all. Apple recently announced their own smart speaker called the HomePod, but at double the price of Google Home and Alexa, will it survive?

Contest Corner
Who Wants To Win A Gift Card?

This month we are giving away (2) $5 McDonalds Gift Cards. The winners will be chosen at random from all correct entries received by the 16th.

Which of these U.S. highways run through Indiana?

A) Route 66 B) Route 1
C) Route 21 D) Route 6

E-mail **Jeff@bssconsulting.com** with your answers!

Business System Solutions

Managing Technology For Your Business

BUSINESS SYSTEM SOLUTIONS
1211 Cumberland Avenue
West Lafayette, IN 47906

Phone: (765) 742-3440
Email: bill@bssconsulting.com

Inside This Issue:

So do not fear, for I am with you; do not be dismayed, for I am your God. I will strengthen you and help you; I will uphold you with my righteous right hand. Isaiah 41:10 NIV