BSSi2

Innovations

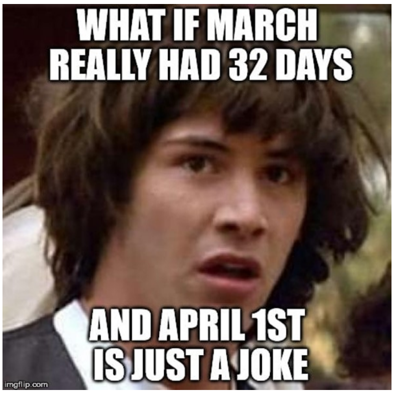
Review Twice, Implement Once. Doing IT Right the First Time.

Scott Bernstein, CPA
President

Nick Espinosa
CIO & Chief Security Fanatic

On the Lighter Side

THE MORNING AFTER THE GOVERNMENT STEALS ONE HOUR OF MY SLEEP


WHAT IF MARCH REALLY HAD 32 DAYS
AND APRIL 1ST IS JUST A JOKE
imgflip.com

Important Cyber Liability Insuring Agreements Checklist (Part 2 of 2) From techrug

Last month we introduced part 1 of a helpful Cyber Liability checklist. This month we are providing the second half of the checklist for you to use as a reference.

There's no hiding it, cyber risks are prevalent. We write about it all the time. As part of your cyber strategy, you need to have cyber insurance, no exceptions. It should be as automatic as car insurance and health insurance. We often get questions about what should it say or cover, or here is what my agent sent me, is this adequate?

We are not insurance experts and we cannot exam every policy that is sent to us. Our standard response will be talk to your cyber insurance agent; if he/she is not an expert in that area, we can refer you to someone who it. That being said, I requested our cyber insurance agent to prepare a checklist of things that a good cyber insurance policy should have. We are including it here and in the next newsletter. It was too long to put in one newsletter (and I want you coming back for more than just the humor). When reviewing this list, keep in mind insurance companies use different terms for the same thing. If the policy has a definitions section, look at that.

> As examples:
> -Everyone is concerned about Ransomware, but policies will probably not use that exact phrase. This checklist uses the term Cyber Extortion.
>
> -You do not see the term HIPAA here as that falls under Privacy Liability.

Typically, my eyes glaze over when I get insurance policies: Very long, lots of terminology that goes over my head, long time to try to read and comprehend. You need a cyber insurance agent you trust to have the right coverage and is an expert in cyber insurance, not just an add-on to the other lines of insurance they may sell. This checklist is a guideline at this point in time to assess the adequacy of the proposed policy.

- Dependent Business Interruption Loss - Income Loss and Extra Expense actually sustained during the Period of Restoration as a result of an actual interruption of the business operations caused by a Dependent Security Breach.
- Data Recovery Costs - Reasonable and necessary costs incurred to regain access to, replace, or restore Data.
- Fraudulent Instruction - The transfer, payment or delivery of Money or Securities as a result of fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions provided by a third party that is intended to mislead through the misrepresentation of a material fact which is relied upon in good faith.

Continued on next page...

… continued from previous page.

- Funds Transfer Fraud - The loss of Money or Securities contained in a Transfer Account at a Financial Institution resulting from fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions by a third party issued to a Financial Institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by the Insured Organization at such institution, without the Insured Organization's knowledge or consent.
- Telephone Fraud - The act of a third party gaining access to and using the Insured Organization's telephone system in an unauthorized manner.
- Computer Hardware Replacement Cost - Includes reasonable and necessary expenses incurred to replace computers or any associated devices or equipment operated by, and either owned by or leased to, the Insured Organization that are unable to function as intended due to corruption or destruction of software or firmware directly resulting from a Security Breach
- Voluntary Shutdown - Crippling global cyber events and attacks cause widespread disruptions. Sometimes it is determined that the best course of action to mitigate potential harm is to shut down their systems. Although this action stopped the spread of malware, it also opened the door to for extra expense and lost income resulting from a voluntary shutdown.
- CryptoJacking - The Unauthorized Access or Use of Computer Systems to mine for Digital Currency that directly results in additional costs incurred for electricity or internet
- Contingent Bodily Injury - Claims wherein the Damages sought by the claimant are for Bodily Injury which arise solely out of a Security Breach affecting Computer Systems
- GDPR Cyber Liability - This coverage is for claims expenses and penalties if a foreign governmental agency or international regulatory body brings an enforcement action against you for a violation of a law protecting the confidentiality and security of Personally Identifiable Information.
- Invoice Manipulation - The release or distribution of any fraudulent invoice or fraudulent payment instruction to a third party as a direct result of a Security Breach or a Data Breach.

Justin Reinmuth is the CEO and founder of techrug (The Technology Risk Underwriting Group). Since 2004, he and his team have had the responsibility of managing risk and customizing over 18,000 policies in areas such as Cyber Liability Insurance, Management Liability Insurance, Commercial Crime Insurance, Business Owners Insurance and Workers' Compensation Insurance. http://www.techrug.com/About.html 800-722-4540

It's Tax Season, IRS Scams are Up

It is that time of year when criminals become aggressive in calling, texting and email about false tax payments due and threatening you with prosecution of you do not "pay up" right then and there. Don't fall for it, do not become a victim. The IRS will NEVER initiate the first contact with a phone call, text or email; it will ALWAYS be in writing on IRS letterhead. This year we have the added complication of COVID-19 stimulus checks and unemployment benefits.

Signs it is a scam

- Caller demands immediate payment, in any fashion. The IRS will never do this.
- They demand payment to other than U.S. Treasury.
- Threatens to immediately bring in the police or law enforcement groups.
- Demand taxes be paid without the opportunity to question or appeal the amount owed.
- An unexpected call about a tax refund.
- Email will provide a link to a site for payment.

What you need to do

- If you need to call the IRS, do not use the phone number on the letterhead.
- Call your tax accountant first. If you do not have one, seek advice and manually go to the IRS web site to get a phone number.
- Record the number and then hang up.
- Report the call to the TIGTA using their IRS Impersonating Scam Reporting form (https://www.treasury.gov/tigta/reportcrime_misconduct.shtml) or call 800-366-4484
- Report the number to phishing@irs.gov and put "IRS Phone Scam" in the subject line.

The old saying: "Only two things are for sure, death and taxes" needs to really be "Only three things are for sure, death, taxes and cyber scams". Don't become a victim.

The IT Services Model Where Everyone Wins – And The One Where You Lose Big

If you're a business owner, there's probably a good chance you spent time figuring out the IT needs of your business. It's not as easy as searching online and picking the cheapest option or the company with the best reviews. The cheap option may not provide the services you need to keep your business at the top of its game, and the best-reviewed business may be too expensive or offer services that are completely unnecessary for your business.

To put it simply, if you want to get the most out of your IT support services, you must do some research. If you haven't spent a lot of time in the world of IT, it can be difficult to figure out where to even begin with your research. If you've found yourself in this situation previously or are preparing to open a new business and are interested in your IT support options, we've got you covered. We've put together the three most common forms of IT support and explain the benefits and drawbacks of each so you can confidently decide on the best option for your business.

Managed IT Services

In this option, the IT services company takes over the role of your in-house IT department for a fixed and agreed-upon monthly rate. They'll install, support and maintain all the users, devices and PCs connected to your network on a routine basis. They will even take care of your hardware and software needs for an extra cost. If you're trying to plan for a monthly budget or want routine maintenance and IT support, this option will work wonders for your business.

It's my sincere belief that the managed IT approach is undoubtedly the most cost-effective and smartest option for any business. With managed IT services, your business will be protected from IT-related problems, and they will keep your systems up and running. They can prevent common "disasters" such as lost devices, hardware failures, fires, natural disasters and a host of other issues that can interrupt or outright destroy your IT infrastructure and the data it holds.

Technology As A Service

Another option that might work really well for your business is using a company that offers technology as a service. With these companies, you'll get everything that managed IT services offer but with the addition of new hardware, software and support. This service ensures that your business is always up-to-date with the newest software and hardware. The greatest benefit of technology as a service is that you'll avoid the heavy cost of new hardware and software when you need it, but you will be paying far more for the same hardware and software over time. You'll also need to pay attention to the services they offer to ensure they can provide what you need and that it does not cost extra.

Time And Materials

Time and materials are often referred to as the "break-fix" method. This essentially means that you pay an agreed-upon hourly rate for a technician to "fix" a problem when something "breaks." It's a simple and straightforward way to pay for IT services but often doesn't work in your favor and can lead you to pay more for basic services. I would only recommend the time-and-materials approach if you already have an IT team and you need additional support for a problem that your current IT team doesn't have the time or expertise to handle. Under the break-fix model, the IT company has no immediate need to stabilize your network because they are getting paid hourly. The break-fix model is unable to supply ongoing maintenance and monitoring, which computer networks need to stay secure.

Business Tidbit

It Isn't Luck, It's SEO – Improve Your Conversion Rates Using SEO

Search engine optimization (SEO) and conversion rates go hand in hand. SEO helps bring people to your website, but conversion rate optimization (CRO) helps make those visits more meaningful. If you aren't getting the desired conversion rates for your website, there are a few tips you can implement to get more from your SEO and CRO.

Speed Up Web Page Load Times: If your website does not load within three seconds, there's a good chance that customers won't wait for your site to load.

Improve Your Visuals With Creative Designs: You want your website to grab a user's attention and encourage them to click through the site.

Utilize Videos And Visual Aids: If users are not staying on your website for a long period of time, add some videos. Users are more likely to stay on your site if there are things for them to watch or look at.

Use Strong Calls To Action: A call to action is a great way to connect with your customer base and will make it easier to track the return on your investments.

March 2022

BSSi2

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

“We make all of your computer problems go away without the cost of a full-time I.T. staff”

"... and Brian, down there, is just here to even out our grid."

CartoonStock.com

Shiny New Gadget of the Month

Desklab Portable Touchscreen Monitor

The pandemic has caused more Americans to start working remotely for their employers than ever before. If you’re working from home, you want to make sure you have the best devices available. One of the best things you can add to make your work more efficient in your remote workplace is another monitor, and there are few monitors out right now that can compete with the Desklab Portable Touchscreen Monitor. This monitor gives you an extra screen to work with as well as a 1080p touchscreen. You’ll be able to expand your desktop, laptop, phone or tablet to become a second portable touchscreen. The monitor is lightweight and requires no setup, so it’s ready to go whenever you need it.

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

f www.facebook.com/NickAEsp

twitter.com/NickAEsp

in www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

f www.facebook.com/bssi2

twitter.com/BSSi2llc