bis TECHNOLOGYGROUP

Consulting Marketing Information Technology Office Equipment

What's New

We are so excited to announce that we have added a few new members to our team.

In the project and purchasing department, we hired Jamie Moyer as the project and purchasing assistant.

In the sales and marketing department, we hired Jasmine Davis as the Inside Sales Pro.

At the help desk, we hired Nichole Fielder as the client concierge.

October 2016

This monthly publication provided courtesy of Phillip Long, CEO of BIS Technology Group.

Our Mission: To deliver solutions to our clients to help them overcome challenges that threaten the health of their business.

Could One Tiny Leak Wipe Out Your Entire Company?

Things were going great at Michael Daugherty's up-and-coming $4 million medical-testing company.

He was a happy man. He ran a good business in a nice place. His Atlanta-based LabMD had about 30 employees and tested blood, urine and tissue samples for urologists. Life was good for this middle-aged businessman from Detroit.

Then, one Tuesday afternoon in May 2008, the phone call came that changed his life. His general manager came in to tell Daugherty about a call he'd just fielded from a man claiming to have nabbed a file full of LabMD patient documents. For a medical business that had to comply with strict federal rules on privacy, this was bad. Very bad.

It turned out that LabMD's billing manager had been using LimeWire file-sharing software to download music. In the process, she'd unwittingly left her documents folder containing the medical records exposed to a public network. A hacker easily found and downloaded LabMD's patient records. And now the fate of Michael's life – and his business – were drastically altered.

What followed was a nightmarish downward spiral for LabMD. Not one to go down without a fight, Michael found himself mired in an escalating number of multiple lawsuits and legal battles with the Federal Trade Commission and other regulators investigating the leak.

Finally, in January 2014, exhausted and out of funds, his business cratering under constant pressure, he gave up the fight and shuttered his company.

One tiny leak that could have easily been prevented took his entire company down. Could this happen to you and your business? Let's take a look at four fatal errors you MUST avoid, to make sure it never does:

Have you developed a false sense of security?

continued on pg2

Please, please, please do NOT think you are immune to a cyber-attack simply because you are not a big company. The fact is, whether you have 12 clients, or 12,000 clients, your data has value to hackers. A simple client profile with name, address and phone number sells for as little as $1 on the black market. Yet add a few details, like credit card and Social Security numbers, and the price can skyrocket – $300 per record is not uncommon. Being small doesn't mean you are immune.

Are you skimping on security to save money? Sure, of course you have a tight budget… So you cut a deal with your marketing manager, who wants to work from home at times. He links into the company network with a VPN. If configured properly, your VPN creates a secure and encrypted tunnel into your network. So his device now links his home network into the company network. The problem is, his home cable modem may be vulnerable to attack, an all-too-common issue with consumer devices. Now you have an open tunnel for malware and viruses to attack your network.

> *"You MUST remove those accounts without delay."*

Could lack of an off-boarding process put your company at risk? It's crucial to keep a record of user accounts for each employee with security privileges. When an employee leaves, you MUST remove those accounts without delay. An internal attack by a disgruntled worker could do serious harm to your business. Be sure to close this loop.

Have you been lax about implementing security policies for desktop computers, mobile devices and the Internet? The greatest threat to your company's data originates not in technology, but in human behavior. It starts before you boot up a single device. In an era of BYOD (bring your own device), for instance, lax behavior by anyone connecting to your network weakens its security. Your team love their smartphones, and with good reason. So it's tough sticking with strict rules about BYOD. But without absolute adherence to a clear policy, you might as well sell your company's secrets on eBay.

Don't let a tiny leak sink your ship – here's what to do next…

Let us run our complete Network Security Audit for you. We'll send our top data security specialist to your location and give you a complete top-to-bottom security analysis with action plan. This is normally a $297 service. It's yours FREE when you call now through the end of October.

Don't wait until disaster strikes. Call 251-410-7601 or e-mail me at jpartin@askbis.com to schedule your FREE Network Security Audit TODAY.

PC and Device Encryption: You've Been Told You Need It, Now Know Why

Introduction

Any company or organization that holds sensitive data has a critical need to ensure that the information stored is properly protected. Businesses that collect personal, private information – data that is used to deliver superior service and make customers' lives that much easier – nevertheless enter into a trust with consumers. In all-too-common cases when data breaches occur and make headlines, reputational damage ensues. And, when data breaches occur in industries where governmental regulations are involved, organizations found to be careless in safeguarding data can also face substantial fines.

In other cases the issue is not customer data but sensitive intellectual property belonging to a company, the secrecy of which is essential to that business' competitive advantage. Proper protection of data can also open the door to new business relationships, especially with institutions that have policies of exclusively selecting vendors and partners that meet certain careful criteria when it comes to data security practices. But in all these cases – whether an organization is incentivized to invest in data security in order to protect their reputation, to meet regulatory requirements, to safeguard intellectual property, to prepare for new business relationships, or for any other reason – data encryption is the first and most critical tool in the data security playbook. Importantly, implementing encryption does not have to be difficult or cumbersome to an organization's operations. In fact, encryption functions best when it is unobtrusive and when it is, more or less, invisible to users.

PC and Device Encryption: You've Been Told You Need It, Now Know Why

You will learn:

- About data breaches that could hurt your company
- How to keep criminals away from your data
- The "nuts and bolts" of encryption
- When encryption is necessary to meet compliance regulations

Claim Your FREE Copy Today at www.askbis.com/encryption.

Anatomy of a Spear Phishing Attack

According to a Trend Micro white paper, "Spear-phishing Email: Most Favored APT Attack Bait," spear phishing can be defined as "highly targeted phishing aimed at specific individuals or groups within an organization." In this way, hackers take more simplistic phishing attacks to the next level, where they have a particular target in mind. Because the cybercriminal knows ahead of time who their victim will be, they can go to extra lengths to personalize and customize the messaging and strategies used in the attack to boost the chances of infection. For instance, Trend Micro noted that oftentimes, spear phishing attacks will include a victim's name and position within the company as opposed to more generic titles and greetings seen in traditional phishing campaigns.

For example, instead of sending a phishing message to attract the attention of anyone within an organization, hackers will include the name of the CEO, as well as his position. This further encourages the target to open the email and download the malicious payload, particularly when the victim has had security training and may know the signs of common phishing messages.

"APT campaigns frequently make use of spear phishing tactics because these are essential to get high-ranking targets to open phishing emails," the TrendLabs APT Research Team noted in the Trend Micro white paper. "These targets may either be sufficiently aware of security best practices to avoid ordinarily phishing emails or may not have the time to read generic-sounding messages."

Spear phishing: What's included in the attack?
According to Trend Micro, a typical spear phishing attack includes an email and an attachment.

The email includes information specific to the target, including his name and rank within the company. This boosts the chances that the victim will carry out all the actions necessary for infection, including opening the email and the included attachment.

The email will also have a legitimate-appearing link or file attachment. These can be a variety of different file types, but Trend Micro researchers found that 70 percent of all attacks feature a .XLS, .PDF, .DOC, .DOCX or .HWP files.

"The file, often a vulnerability exploit, installs a malware in a compromised computer," the white paper stated. "The malware then accesses a malicious command-and-control (C&C) server to await instructions from a remote user. At the same time, it usually drops a decoy document that will open when the malware or exploit runs to hide malicious activity."

Because executable files can look suspicious to some users – especially those who have had security training in the past – hackers will disguise these with fraudulent icons and include unnecessary spaces in the file name to camouflage the .EXE file name extension.

The vast majority of spear phishing attacks utilize this approach – Trend Micro monitoring showed that 94 percent of emails include malicious file attachments. The remainder leverage other strategies like encouraging victims to click malicious links to download malware and exploits.

Protecting Against Spear Phishing
Although spear phishing messages can be challenging to recognize in the flood of corporate emails, and are designed to specifically take advantage of this, there are things companies can do to lessen their chances of infection.

In addition to keeping an eye out for suspicious looking messages, links and attachments, it's also important to consider the sender. Company employees and executives should not open emails or download attachments from any unfamiliar sender. This could be a telling sign of cybercriminal activity.

It's also critical to keep track of what data is accessible from different platforms.

"Organizations should strive to improve their existing defenses and take into careful consideration what types of and how much information they make available online," the white paper stated.

Businesses should also have the right protection systems in place to help mitigate these types of threats. This no-maintenance system includes security measures to specifically prevent spam, phishing and malware. BIS can help! Call 251-410-7601 today!

-Noah Garner

The Case for Employee Monitoring

By: Taylor D’Amico, Digital Marketing Specialist

While this is a controversial issue for some. The fact remains that the ability to checkup on employees’ computer usage is crucial for network security.

Before any further discussion on the benefits of employee monitoring, we must point out how imperative it is for a company to have all employees sign off on a computer use and monitoring policy.

Laws have traditionally been on the company’s side when it comes to computer surveillance, but employee morale and trust will soon dwindle if employees feel kept in the dark about what employers are looking at and why.

It’s understood that no one likes to be micromanaged. However, monitoring workers gives companies a multitude of benefits. This is one of the main reasons why employers have the broad legal latitude to track what workers are doing on their network. Most states don’t require employers to notify employees if they are monitoring, but recent bills have been introduced into state legislatures that would make it mandatory for companies to alert their employees.

To avoid any potential backlash, we suggest putting in place a clear and conspicuous Acceptable Use Policy (AUP) that all employees must sign that explicitly states what is being monitored.

Take a look at these statistics for an overview of how globally popular this practice is becoming:

63% of US employers monitor their employees Internet connections.

64% of employees use the web for personal reasons during work hours.

77% of major US companies monitor employees at work through:

1. Email
2. Web browsing
3. Phone calls
4. Computer files
5. Video recordings

Monitoring by management has uncovered such nefarious conduct as prostitution, gambling, and theft that occurred during business hours. Other companies have discovered enormous amounts of time spent watching cat videos on YouTube and eBay shopping. Employee hijinks in cyberspace can cause trouble for a corporation beyond the activities of pornography or online shopping. For example, inappropriate social media posts can involve the company in expensive lawsuits or create PR headaches that can severely damage a company’s reputation.

More and more companies are creating Social Media Disclosure policies for employees to sign. These policies outline what can and cannot be posted about the employer online, thereby preventing employees from tarnishing the name of the company they work for and discussing other proprietary or private information on their personal accounts. In these policies, employers also outline whether employees can access social media at work or on company devices.

So for a business, the benefits of having a proactive arsenal of security software tactics that are deployed continually to protect your sensitive data and network is hopefully evident.

Business Information Solutions, Inc. now offers security and compliance training for your employees. With our in depth courses, your staff can stay educated on how to avoid the vast potential threats and learn hands on from simulated attacks. Contact us today to schedule a free consultation and demo of our products and services.

Get Your FREE Network Evaluation!

Give us a call to schedule it… 251-410-7601!

Shiny New Gadget Of The Month:

Hololens: Your New Reality?

A game designer sees a moving 3-D image of a living, breathing, mace-wielding ogre – on her desk. She flicks a finger and he turns from side to side, giving her a full view of his outfit and weapons belt.

An architect looks up at the ceiling in a building he’s just designed. He waves his hand and reshapes it, allowing more light through. All virtually.

A space scientist designing a Mars rover strolls through the landscape, noting from all sides the position, shape and size of rocks his vehicle must navigate.

Now it’s your turn. Put on the new HoloLens by Microsoft, and what do you see? How could you use this cool new augmented reality (AR) tool in your business?

At $3,000 for the developer’s version, it may not be an impulse buy. But new AR tools like this will soon be part of your computing world.

4 Mistakes to Avoid When Using SEO

By: Taylor D’Amico, Digital Marketing Specialist at BIS Designs

Here’s a quick overview of the top mistakes to avoid when leveraging SEO for your company’s best success online.

1. **Keyword Stuffing.** This used to be a regular technique in search engine optimization where a webpage had “keywords” (popular words used in search queries) placed all over the site in metatags or in the content. However, Google soon realized that the number of keywords on a site did not necessarily equate to a valuable resource for the web user. Currently, keyword stuffing is viewed as a black hat technique and an attempt to manipulate a site’s rankings in search results. This can potentially cause a site to be banned or penalized in search engine rankings.

2. Keyword Research or Lack Thereof. Many companies these days are telling people to just write naturally and not worry about keywords, but there is a deep value in using the search algorithms to your advantage. Having quality content on a website is the leading factor for making a website useful and popular for visitors. Keywords need to be researched and selected first before any writing begins in order for the content to read naturally.

3. Not Using Long Tailed Keywords. Long tail keywords, or descriptive phrases, are keywords too. They are much more likely to rank well in search results than short tail keywords. Why? Because people are getting much more specific in their searches, and keyword optimization should follow suit. You may get fewer hits, but the hits you get will be from web users that are much further down the road towards taking action than those that were only searching for one general word. It’s also much more achievable to get a webpage to rank highly on the search engine listings for long tail keywords because the competition is not as high as it is for general one word terms. Just think about the intention difference between someone searching for “Mobile Bay” versus “Mobile Bay charter boat tours Fairhope AL”. The specific search query is more likely to reflect a shopper who knows what they’re looking for and is closer to a purchase decision.

4. Not Adding Fresh Content to Your Site. Okay, so now you have a stellar website with dynamic content and optimized keywords ready to rock the socks off of users. But before you expect to be listed on that first page of search results on Google, and ideally the top three listings, you need to understand the importance of updating the content on your site regularly. If you’re not regularly updating your website, search engines are not going to continually notice you. Each time you add something new to your site, it’s a beacon calling the web crawling search bots to come back around to index your site, which in turn gives you better chances of higher search rankings.

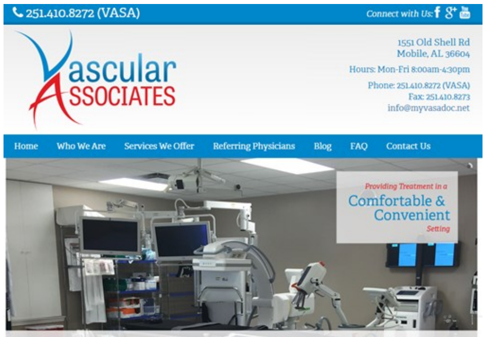
Our SEO & Online Specialist will collaborate with you to create the most effective search engine optimization strategy possible, customized to your individual needs. Bring your website into the modern competitive arena with strategic SEO services from BIS Designs.

Is Your Marketing On Track?

Give us a call now to set up your FREE marketing roadmap assessment! Call 251-410-7601!

Website of the Month

Vascular Associates



Vascular Associates holds the distinction of being Alabama’s first office-based setting for direct treatment inside arteries or veins without requiring incisions.

To visit their website, go to http://myvasadoc.net/.

> ***“We don’t have a choice on whether we DO social media, the question is how well we DO it.”***
>
> *-Erik Qualman*

Dealing With The Dark Side Of Social Media

Social media has become a true amplifier, permeating every nook and cranny of the web, giving a megaphone to those who might have previously found themselves voiceless.

While I generally believe that the proliferation of the social web is a good thing, it does have a dark side that is difficult, if not impossible, to ignore.

I was reminded of this recently when an unscrupulous competitor accused me and my friend Larry Winget of an ugly racial slur. While it was totally fabricated, this person willfully resorted to defamation of character to defend his indefensible behavior.

It's easy to get mad, get on your computer and allow emotions to run amok. And that can come back to bite you. Yet there are times you shouldn't acquiesce to digital bullies. You need to take a stand.

Here are a few tips on how to keep your social media actions in check, and how to react to others who just can't seem to control theirs:

How do I think through my social media actions in a heated moment?

If you wouldn't say it to your grandmother, don't write it on Twitter. It feels good to blast an opponent, but such outbursts can easily be used against you.

Remember that everything you say or do on the web is archived. Consider everything you write on the Internet to be permanent. Trolls may delete their comments, but they still leave a trail.

Still debating saying it? Sleep on it. If you really feel the need to say something that might be taken the wrong way, consider sitting on it overnight. Waiting until the next day will rarely hurt your point, and it may save huge amounts of embarrassment.

If you do say it…make sure you feel you could defend it in a court of law. Falsely accusing someone of something is a big deal, and the repercussions could amplify beyond your original intentions.

How do I react when I am targeted on social media?

Grab screenshots. If someone truly is going after you, the first move is to gather evidence. Make sure you have copies. Odds are that they will quickly realize what they have done and will try to erase their trail, so the best thing you can do is make sure you have a copy on hand.

Report them. Twitter, LinkedIn, Facebook and most other platforms have guards against those who harass others. Don't hesitate to put in a report – that's why those guards are there!

Remember that the truth is your best defense. As someone who has been egregiously accused of something I did not do, I took solace in the fact that I was innocent, and as such the accusation cruelly asserted could never be proven.

We live in a world where unscrupulous people have migrated to online communities and live among the rest of us. I hope you never have to use the above actions, but when you do, I hope they serve you well.

Mark Sanborn, CSP, CPAE, is president of Sanborn & Associates, Inc., an idea studio dedicated to developing leaders in business and in life. Mark is an international best-selling author and noted authority on leadership, team-building, customer service and change. Mark is the author of 8 books, including the best seller The Fred Factor: How Passion in Your Work and Life Can Turn the Ordinary into the Extraordinary, which has sold more than 1.6 million copies internationally. Learn more about Mark at www.marksanborn.com.

Considering Facebook Live Video for Your Business?

Using Facebook Live is brain-dead simple. If you haven't already, install the Facebook app on your smartphone. Open it up, tap the red "Go Live" icon and you're on. It tells you how many are watching, plus their names and comments. When you're done, it saves to your Timeline. And, unlike Snapchat or Periscope, it doesn't disappear after just 24 hours. You can share, embed, Tweet – or delete – to your heart's content. And you can filter who sees it. As for content? Interview key employees, big shots in your niche or your customers. Share how you're making a new product. Or how your team relaxes. Why do it? Your customers love getting that little peek "behind the scenes."

-*PostPlanner.com*

Help Us "Hook" Some More Clients Like You & Get Rewarded!

We've decided to start a special rewards program for the clients we value the most.

Here's the deal...

Refer clients to us and receive a $50 gift card to any place of your choosin' when your referral becomes a BIS client. Earn a $100 gift card when 3 or more of your referrals do business with BIS!

For more information, visit www.askbis.com/referral or call 251.923.4015.

*The BIS Division Only

"The strength of the team is each individual. The strength of each member is the team."

-Phil Jackson

Who Wants To Win A $5 Starbucks Gift Card?

Every week, we will have a Grand-Prize Winner for our Monthly Trivia Challenge Quiz! He or she has to be the first person to correctly answer my quiz question.

Last month's trivia answer was b) Whiskey - the product that the term "brand name" originated.

Now, here's this month's trivia question. The winner will receive a $5 gift card to Starbucks!

Which Halloween custom began as a way of finding out who would get married first?

a) Trick or treating
b) Making lanterns
c) Bobbing for apples

Email us right now with your answer!

hvalentine@askbis.com

Want to Know the Secret to Beating Ransomware?

If there's one pop-up you NEVER want to see on your computer screen, it's this: "Your files have been encrypted. You have 72 hours to submit payment or they will be deleted forever." Once ransomware hits, it's too late. Game over. The best way to beat ransomware is prevention. Make sure it never happens in the first place. And if somehow it happens anyway, make sure you have up-to-date backups ready to go. The first step to prevention is to invest in serious cybersecurity. Start with antivirus software with active monitoring. Then, layer in anti-malware and anti-ransomware programs. Finally, store current backups in the cloud and/or on a separate unplugged hard drive.

-blog.malwarebytes.com

The ONLY business educational program on the Gulf Coast that's FREE and will educate your company on business best practices, information technology, office equipment, web design and digital marketing

October Events

Oct. 27th at 11:30 AM

Bamboo Steakhouse & Sushi Bar

Mobile, AL 36695

Cybersecurity Seminar (FREE!)

Learn the six critical IT security protections every business must have in place now to avoid cyber attacks, data breach lawsuits, bank fraud and compliance penalties.

www.askbis.com/seminar

To RSVP for any of these events, call 251-923-4015 or visit www.bisuniversity.com.