TECHNOLOGY INSIDER

"The latest in technology news, trends & tips for business"

Our Mission:

At BoxMeta, we are committed to providing valuable, no-nonsense, quality technology services and solutions to our clients. We will understand our clients' goals and help accomplish them through simple and affordable technology solutions.

Win a FREE Cybersecurity Seminar

Email 'November Offer' to: events@boxmeta.com for a chance to win a FREE Cybersecurity seminar for your company!! *(minimum 10 employees)*

What's Inside:

Could One Tiny Leak Wipe Out Your Entire Company?

Things were going great at Michael Daugherty's $4 million medical testing company. He was a happy man. His Atlanta based LabMD had about 30 employees. Life was good.

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 to download music. In the process, she'd unknowingly 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 downward spiral for LabMD. Michael found himself mired in an escalating number of lawsuits and legal battles with the FTC and other regulators. Finally, in January 2014, he gave up the fight and shuttered his company.

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:

1.   Have you developed a false sense of security? 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.

2.   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 without a VPN (VPN creates a secure and encrypted tunnel into your network). So his home 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.

3.   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.

4.   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. Without absolute adherence to a clear BYOD policy, your company's secrets are at risk.

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

Call BoxMeta today to sign up for our FREE Technology Assessment
904-229-0922

Gadget of the Month

HP Sprocket Portable Photo Printer

Printing photos has never been easier from your smartphone. Connect your social media accounts to the free HP Sprocket App. Open the top of the printer, drop the paper in, and start printing. Sprocket uses seamless Bluetooth connectivity. It easily fits into any bag, so you can create 2x3-inch stick-able snapshots whenever the moment strikes.

Cost: $130 on Amazon + $10 for 20 sheets of HP ZINK Sticky-Backed Photo Paper

Who Wants to Win a $25 Gift Card?

The first person to answer correction will win a $25 Gift Card.
Email your answer to:
trivia@boxmeta.com

Take the number 30, divide it by 1/2, and then add 10. What # do you get?

Business Briefings

Windows Vista End of Life. Windows 7 is up next...

Windows Vista support will end on April 11, 2017. As of October 31st, Windows 7 can no longer be purchased pre-installed and end of life is projected for January 2020..Call Boxmeta if you haven't already upgraded to Windows 10. It may not be too late to upgrade for FREE.

Ditch the meeting, get more done.

The average manager spends 30%-50% of their time in meetings. Most feel 67% of meetings are a waste of time. So what can we do to stop killing time? Here are three ways to tell if a meeting is worthwhile. 1) Tally the number of attendees cost based on average pay rate and time spent at the meeting. Is the desired outcome worth more than the cost? 2) Will this be a one-sided affair? A dead giveaway is the conference call when the boss puts everyone else on mute. 3) Is the meeting a guise for "communication"? Instead, send an e-mail, point to a website or suggest someone to consult with. Now you're talking...

-Entrepreneur

The Day the Internet went down..Will It Happen Again?

On October 21st we woke up to find that several mainstream web sites such as PayPal, Twitter, Amazon, Netflix, Spotify, CNN, NYT, etc were down. Dyn, an internet infrastructure company, experienced a massive Denial of Service (DDoS) attack. The attack used a 'botnet' of THOUSANDS of Internet of Things (IoT was covered in the BoxMeta September newsletter) devices to flood Dyn's servers. Estimates are that between 13b-18b IoT devices are now in use. Webcams and DVR's were the primary devices utilized in this attack. Security experts were not surprised by this event and believe it's not the last. The Online Trust Association (OTA) has asserted the attack could have been easily prevented if the manufacturers of these devices had built-in better security protocols to their products. Among the most critical IoT vulnerabilities are: discoverable administrative controls, default passwords and no capability for the software to be patched or updated. Analysts doubt this was the work of a large criminal network or state but instead more amateur criminals that used the 'Mirai' malware source code after finding it publicly posted on a hack forum website.

If you have ANY device that has access to or can be accessed from the internet, make sure to change default settings & access codes. Update & Patch if possible.

2 Types of Identify Verification Explained:

While everyone knows how important their online security is, they may not know what types of online security are best, nor the differences between the most commonly available options. There are two security authentication measures that are quite similar in name and that are often used. These are known as two-factor authentication and two-step authentication.

Most people and businesses use the terms two-step and two-factor authentication interchangeably. There are, however, subtle differences between the two.

A **two-step authentication** process requires a single-factor login (such as a memorized password or biometric reading) as well as another of the same type of login that is essentially sent to the user, such as a one-time-use code on your cell phone as the second step. Both are "something you know". Two-step authentication is more secure than a single-step authentication (i.e. just the password), however, if a person or business is

hacked, it will do only a little to stop hackers from getting a hold of whatever they are looking for.

On the other hand, there is **two-factor authentication,** which is significantly more secure. It requires two different types of information to authenticate. For example, it could be a combination of a fingerprint ("something you are") as well as a password ("something you know"). Because the types of information are different, it would require a hacker a great deal more effort to obtain both forms of authentication. It may also consist of swiping a keycard in a door-locking mechanism ("something you have") and then a fingerprint scanner ("something you are").

In essence, every two-factor authentication is a two-step authentication process, but the opposite is not true.

No site or product is 100% secure. Keep those in the vault above your shoulders. ***Remember, if someone can get to your email they can reset your site passwords..