Excalibur TECHNOLOGY
www.excaltech.com • [877] NET - KING

TECHBytes
July 2017

"When it HAS to work, call Excalibur Technology!"

In This Issue:

You Will Soon Be Able to Search the Web With Your Smartphone Camera, Thanks to Google Lens

While many instances of augmented reality may seem gimmicky, Google is taking strides toward making AR a purposeful utility in our mobile devices. This was made apparent when Google's CEO, Sundar Pichai, announced Google

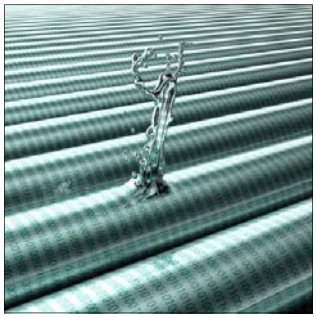
Read the Rest Online! http://bit.ly/2tKVmxK

About Excalibur Technology Corp.

Business owners demand simple, reliable and powerful technology solutions to keep them ahead of their competition while reducing their costs; solutions that require expertise, teamwork and dedication. Excalibur Technology has built a reputation for excelling at helping our business clients achieve these goals.

Visit us **online** at:
www.excaltech.com

What's Your Personal Information Worth On The Black Market? It's All About Supply And Demand



If your company's sensitive data was to be put up for sale, how much do you think it would go for? Chances are, you may be guessing a little high, which makes things worse for businesses in such a situation. Assuming that your data will be sold for a premium price will likely lead you to believe that fewer criminals will access it than actually will.

How to Sell Stolen Data

Since selling stolen data is illegal, the favored place to put it up for sale is the dark web. This is because the dark web can only be accessed through special software that hides the user's identity, and requires all transactions to be made in Bitcoin. This way, illegal items can be sold like any item on a typical merchant website would, including ratings provided by previous buyers.

These illegal items that are put up for sale are usually the kinds of things that criminals would find useful. This includes cyber criminals, who will exchange cryptocurrency for stolen data. For example, let's say for a moment that your company had fallen victim to a cybercriminal who had managed to steal corporate bank account credentials and credit card info from a variety of businesses.

This cybercriminal could set up a seller's page where potential buyers could place an order for data, charging these buyers based on what specific information they wanted.

(Continued on page 2)

Here Are Your Options For Managing Mobile Devices In The Workplace

Did you know that, according to Gartner, a whole 80 percent of all employees bring their personal mobile devices to the office? It's a rather troubling development for business owners who want to secure their data and keep their employees productive. However, this Bring Your Own Device (BYOD) trend has proved extremely beneficial for prepared organizations. This must prompt the question of how your business manages mobile devices in the workplace.

The usual response to mobile devices appearing in offices is either the employer supplying company devices, or preventing their use altogether. Unfortunately, neither of these are all positive, so it's best to approach the situation with an informed and open mind. What follows are the circumstances that come with each approach.

Company-Provided Mobile Devices

Depending on the kind of work your organization does, providing company devices might be beneficial for employees. However, you'll need to consider all of the finer details, including which platform the devices run on (iOS, Android, Windows), contract terms, and how your organization plans on controlling and protecting data located on the devices. Creating a policy that clearly outlines how work and personal information is separated on the device, the privileges that the employee has with the device, a plan if the device is ever misplaced, and what happens when the employee quits, is the key to guaranteeing data security.

(Continued on page 3)

What's Your Personal Information Worth On The Black Market? It's All About Supply And Demand

(Continued from page 1)

For instance, the buyer could be interested in cards provided by Discover, and specify that in their order. What's more, they could specify whether or not they wanted the security codes (the login credentials that the card was associated with), the date the card expires, where the card has been used, the name the card is under and that person's date of birth, credit score, and even their mother's maiden name. These variables influence the cost, as once the transaction is complete, the data is ready to be downloaded.

How Much Data Costs

Even illegal markets are subject to the laws of economics. For instance, the concept of scarcity dictates that the less of a good that is available, the higher its value, and vice versa. This is true even of stolen data--and because the market for stolen data changes pretty quickly, these prices are apt to change very quickly as well.

However, that does not mean that it is impossible to get a feel for the what is generally charged for stolen data. For instance, purchasing the comprehensive data for a stolen credit card (described as "fullz" in dark web slang) will set someone back by some amount between $13 and $21.

Depending on the data up for sale, pricing can vary as well. Financial accounts are priced based on their contents--an account holding $2,000 might cost a cybercriminal $100, and an account that holds $15,000 might cost the buyer $1,000. Recent events have caused a drop in the prices of compromised electronic medical records, so what would once cost about $350 now costs around $100.

Why It Matters

Consider, once again, the cost of stolen credit card credentials. If all a criminal needs is $13 to purchase stolen credit card data, it stands to reason that more credit cards will be sold, feeding back into the demand to steal more credit card data. These credentials have to come from somewhere, after all, so many cybercriminals will look to replenish their stock of credit card data; often targeting businesses. How well protected is yours?

Remember, most cybercriminals are looking for the easy target to steal data from. Excalibur Technology can help keep you from being the easy target. Give us a call at (877) NET - KING to keep your data safe.

Share this Article!
http://bit.ly/2uD60nq

3 Reasons Why BDR Is The Best Way To Backup Your Company's Data

If we asked you how you back up your data, would you be able to respond with enough knowledge to seriously talk about the topic? Many small organizations are under the impression that data backup is only necessary if your business suffers from a data breach or data loss incident. However, the truth is that if you want to ensure the future of your business, data backup is absolutely crucial.

However, tape backup can only do so much. While tape backup is certainly better than no backup at all, it takes much more than tape to properly secure your data infrastructure from harm. If you want a truly dynamic solution, Backup and Disaster Recovery (BDR) is the ideal choice. All it takes is a stroke of bad luck to cause even a hint of data loss, so you should do all that you can to preserve your organization through any means necessary.

BDR Provides an Ideal Recovery Point Objective

Your recovery point objective should be one that allows for the minimal amount of data loss. In other words, how recent your last backup was, has a lot to do with meeting this objective. The last thing that you want to ask yourself is how much data you're willing to part with in the event of a data loss incident.

The bottom line is that no amount of loss is acceptable, but tape backup doesn't allow for this. You could potentially lose out on an entire day's worth of progress due to the fact that tape backup must be performed after hours. Instead of suffering this loss, cloud-based BDR can take backups as often as every fifteen minutes. These snapshots only capture what has changed on your network since the last one was taken, so operations are no longer interrupted just to back up a file.

BDR Offers a Faster Recovery Speed

Tape backups can take anywhere from a couple of hours to an entire day to completely deploy, which means that you'll experience more downtime than you might initially think. If you take this amount of time and multiply it by the number of employees you have, the costs can add up pretty quickly, breaking your budget and making it more difficult to recover. Cloud-based BDR can help your organization get back in business following a data disaster with minimal downtime. You won't have to worry about finding a device to get back online, as the BDR device itself can be used in place of a server as a temporary replacement while you get your act together.

BDR Uses Off-Site Storage

If you use tape backup, where do you store the tapes? Some organizations like to keep them on-site, but this places…

Read the Rest Online!
http://bit.ly/2tLn25m

Here Are Your Options For Managing Mobile Devices In The Workplace

(Continued from page 1)

Unfortunately, this is often seen as a quick fix. You are spending money and forcing your employees to comply with the rules, but this doesn't fix the problem of controlling data on its own. Statistics also show that employees aren't particularly unhappy about company-owned devices, but that the solution can feel like a slap in the face to employees who work well using their own personal devices. On the other hand, some staff might feel excited about a brand new smartphone on the company's budget, so it's up to you to determine what the best approach to this situation is.

Banning Personal Devices Altogether

Some employers will just fully ban access to personal devices, which means that any employee using them for any reason will be written up or face similar consequences. While this can protect your data, this will likely create a rift between your employees and management.

You might only be trying to protect your data, but they'll only see this as management making their jobs more difficult. While this doesn't necessarily happen all the time, it's still often enough to cause concern. It's also problematic for your organization, as mobility is likely something that your competitors have considered implementing themselves.

Thankfully, There Are Options

If you can meet your employees in the middle ground of this sensitive topic, they'll be thankful for it. By this, we mean taking the time to discuss data security with your employees while allowing them to use their own personal devices, so long as they abide by your protocol.

Employers have the opportunity to push policies such as including some type of authentication on their devices (passwords, pins, patterns, etc), alongside secondary measures such as two-factor authentication on accounts located on the device. Providing the employer with the rights to revoke access to email and the ability to wipe data in the event of a stolen device must also be a point of discussion.

Laptops brought from home should be outfitted with company antivirus protection and remote monitoring, along with the ability to set up a VPN or hosted desktop solution so that there's no need to worry about what sorry state the device is in. This can also make it easier to solve troubles with software licensing and accessing company data while on a public Wi-Fi connection.

The best way to approach personal mobile devices in the office is by implementing a BYOD strategy. This should be capable of responding to any and all security discrepancies that may arise from mobile devices being used for work purposes. If you're having trouble putting together such a policy, it's in your best interest to reach out to professional technicians for consultation. Excalibur Technology can help your organization put together a solid BYOD policy that keeps your data secure. To learn more, reach out to us at (877) NET - KING.

Share this Article!
http://bit.ly/2v0vywZ

How Buying Bargain Technology Will Hurt Your Company In The Long Run

A responsible business owner looks at the repercussions of their actions, however, it's not always easy to determine what the right action is. Something to keep in mind is that, if it benefits the long-term mission of your organization, chances are that it's the right thing to do--especially with technology solutions.

For an example, let's take a look at the procurement process for new technology acquisitions. Some laptops will run a price tag of $200, while more advanced models could extend up into the thousand-dollar mark. It's important to remember that when buying new technology, a higher price tag generally means that you'll be purchasing something that's more reliable, more powerful, and more functional.

However, those that are too focused on short-term decision making will wind up staring at that price tag and questioning their decisions. They might choose to go for the less expensive model in order to save some cash in the short-term, but this could be a big mistake.

Administrators and managers who go all-in on new hardware don't just do so for bragging rights--they do so because it's certainly worth the cost in the long run. Reliable technology is invaluable, especially if workers can't do their jobs because their technology solutions don't work properly, you'll feel it in your budget. Investing in quality hardware can help you avoid this issue entirely.

You can apply this train of thought to how technology can affect employee productivity, along with their morale. If they are using inexpensive hardware in an attempt to save some money in the budget, chances are that they will know--especially when the hardware breaks down frequently and they have to deal with frustrating downtime.

A short-term thinker might not see this as a problem, as they believe their workers can suffer through it and appreciate what has been given to them to do the job they are paid to do. However, a…

Read the Rest Online!
http://bit.ly/2uYLike

Advice For Passing Your Next IT Audit With Flying Colors

Most people think of audits and immediately cringe, but the fact of the matter is that businesses wanting to maximize output can really benefit from an audit. Audits can be great ways to ensure that a business' priorities are being given their due attention, and that best practices are being utilized. An audit of your IT infrastructure and network can go a long way toward helping you determine if there are changes you need to make in order to maximize the profitability of your organization.

Here are three of the most common problems that our engineers find when conducting our comprehensive IT audits.

Outdated Software

It doesn't matter if it's the operating system on your workstations or the software on the servers, if you fail to apply critical updates and security patches to your operating systems, then your network will be vulnerable. This is a big red flag during any IT audit. Since outdated versions of software can become problematic for your integrated security protocols, by not properly updating your mission-critical software, you could be putting your business at significant risk.

An Absent Business Continuity Plan

As a part of a risk management strategy, any organization that doesn't have a business continuity plan is ignoring the truth. The facts suggest that a disaster could happen at any moment, whether a company is ready or not. If you fail to prepare for a disaster, you're staring failure in the face.

Poor or Lackluster Implementation

When it comes to regulatory compliance, Excalibur Technology will audit your internal processes, and analyze how they could be more efficient or secure. If you have outdated IT policies, they can end up costing you a lot more than a passing grade on an IT audit. If you haven't properly tested your infrastructure, or if you've failed to deploy modern security best practices like multi-factor authentication, then your organization will perform poorly on an IT audit.

Furthermore, if an auditor sees that your organization's IT department splits responsibilities on a per-task basis, you'll be more likely to score lower than if all IT resources understood how to perform every task necessary to their position.

These are only a few ways that your company could fail to perform as intended during an IT audit. If you want to ensure that your organization can pass your next audit, then you'll want to ensure that your IT understands the importance of adhering to security best practices and industry standards.

Lastly, it is incredibly important that you remember that auditors aren't the ones who are trying to sink your business. If anything, they are attempting to help you improve the way your organization operates. They are simply doing what your IT department should be doing in the first place by checking to see if you have unpatched or vulnerable systems, or aren't adhering to best practices.

Excalibur Technology can help your business ensure its security by performing an IT audit. We can comb through your network for any potential issues and suggest ways to resolve them. To learn more, reach out to us at (877) NET - KING.

Share this Article!
http://bit.ly/2w1jBo1

WE HAVE MOVED OUR DATA CENTER!

We are excited to announce that we moved our data center operations into our new facility on July 22, 2017. This is a high quality, Tier 3, fully secure SOC2 Type 2 compliant and audited facility. This new facility offers our clients:

- Increased Security
- Redundancy in Power and Cooling
- Higher Availability
- Increased Bandwidth Availability & Redundancy

All Hosted Servers and NOC services are now running from this facility. Call us with any questions or to setup new service!

Excalibur Technology Corp.

Barrington, IL
Clearwater, FL

Toll-Free: 877-NET-KING

Visit us **online** at:
www.excaltech.com

facebook.excaltech.com
linkedin.excaltech.com
twitter.excaltech.com
blog.excaltech.com
support@excaltech.com