The Tech chronicle

Creative Consultants Group, Inc. October 2017

What You Can Learn From Equifax's Leak

When it comes to security, it's better to be safe than sorry. But as the Equifax leak case has taught us, once a security breach *does* happen, it's best not to be sorry *twice.* Read on so your business doesn't experience the same fate as the giant, bumbling credit bureau.

Read More

October 2017

CREATIVE CONSULTANTS GROUP

This monthly publication provided courtesy of Bill Hinson, CEO of Creative Consultants Group, Inc.

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

You're Better Off Giving Your Employees A $1,000 Bonus Than Being Cheap With Technology

Imagine, for a minute, that you're the CEO of a scrappy, promising new start-up. In the beginning, it was just you and two other employees working on dinky PCs out of a 12-by-12-foot office, but times are picking up and the company is heading into the uncharted waters of rapid growth.

As the business moves into the public eye — and, in turn, the hungry eyes of potential hackers — it's become obvious that you're going to need to lock down your data. At this critical stage, a cyber-attack could mean the death of everything you and your team have built.

But the budget is looking lean. Everything you've done so far has been by the skin of your teeth, so why should security be any different? You put one of your more tech-savvy employees on the case, tasking him with finding the cheapest cyber security solutions available. Sure, he may not be an expert, but he understands computers. What could go wrong?

He scours the web, perusing dozens of "Top 5 Cheap Firewall Software" articles, and, with the help of a scrappy how-to guide, installs what seems to be the best of the lot on your servers and across all your computers. The entire process takes 10 hours, and costs the company next to nothing.

Potential crisis averted, you turn your attention to other matters. We'll revisit our cyber security later, you think, once we have a little more financial wiggle room.

Across the following year, the company's success skyrockets. The phone is ringing off the hook, new

Continued on page 2

business is flooding in and your profit margin is exploding. You even ended up snagging a feature in Entrepreneur magazine. Your company is the envy of all your peers.

That is, until the day that you get hacked. One morning, an advanced strain of ransomware easily sidesteps your free antivirus and starts wreaking havoc. It slithers through your systems and locks you out of everything, from client data to basic Word documents, and encrypts it behind a paywall, demanding $50,000 in Bitcoin or you'll lose access to all of it — forever.

You couldn't make room in your budget for a robust cyber security solution. Well, how does that $50K ransom strike you?

This may sound like nothing more than a horror story, but in reality, this happens to business owners all over the world each and every day. An IBM security study from last December discovered that over half of businesses surveyed had paid over $10,000 in ransomware payoffs, with 20% paying over $40,000. And that's not even including the millions of dollars of damage caused by other forms of malicious software every year.

The fact is, when your time, money and business are on the line, it simply doesn't pay to be cheap when choosing your cyber security technology.

> **"The fact is, when your time, money and business are on the line, it simply doesn't pay to be cheap when choosing your cyber security technology."**

Think of it this way. Say, with your free antivirus, you're "saving" $100 a month. Lo and behold, a virus manages to punch its way through and causes chaos throughout the company server. Even if you're lucky and it isn't ransomware, by the time you've managed to expunge the stubborn virus from your business, you'll have put in countless man-hours, guaranteed to cost you more than that $100 a month. Instead of throwing those thousands of dollars down the drain, you'd be better off giving each of your employees a $1,000 bonus!

Free antivirus software, giveaway cyber-protection, or a $5 firewall seems like a great idea, until a hacker cuts through your company's defenses like a warm knife through butter. These guys love when they see these outdated, cheapo barriers guarding your priceless data — those are the paper-thin defenses that keep hackers in business.

You wouldn't buy a rusty, secondhand old lock for your house, so why are you installing primitive cyber security software to protect your most precious company resources?

In today's world of rampant cybercrime, it's inevitable that somebody will come knocking at your digital door. When that day comes, do you want a free piece of software that you saw on LifeHacker, or a tried-and-tested, up-to-the-minute, comprehensive security solution?

Don't be shortsighted and risk everything just to save a quick buck. Invest in your company's future, and protect yourself with the most powerful tools on the market. Call us at **(843) 234-9980** and allow our skilled consultants assist you with your network security.

CCG's Free Executive Brief Reveals The Top 10 Ways Hackers Get Around Your Firewall & Antivirus To Rob You Blind

The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This report reveals the most common ways that hackers get in and how to protect yourself today.

CREATIVE CONSULTANTS GROUP

Creative Consultants Group, Inc.
Bill Hinson, CEO
PO Box 444
759 Century Circle
Conway, SC 29526
www.getccg.com
(843)234.9980

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This report reveals the most common ways that hackers get in and how to protect yourself today.

To Claim Your Free Report, Visit
www.getccg.com/10ways/

Shiny New Gadget Of The Month:

Picture Keeper Connect, The Best Way To Back Up Photos On The Go

Nothing feels worse than having to delete an old favorite to make room for some new photos. The Picture Keeper Connect solves both of these issues, providing easy-to-use backup for your phone or tablet.

The Picture Keeper Connect, which looks a lot like a conventional flash drive, is designed specifically to back up photos, videos and contact information with just a couple of button presses. It plugs into your phone and gets to work. Even better, it can do all of this without the need for WiFi or network connection. It keeps your photos in their designated album, meaning you won't end up with a cluttered mass of photos when you transfer them to a new device.

Simple, functional, and portable, the Picture Keeper Connect is a must for any avid smartphone photographer.

A Diverse Team Is More Productive

Everyone knows the saying, "If you build it, they will come," from the 1989 film Field Of Dreams. Well, the same rule applies to the type of work environment you create, and, as a result, how diverse your team becomes.

Diversity may not happen overnight, but you can be sure that a diverse team means a broader range of perspectives brought to the problem-solving table. When employees feel accepted and comfortable in their workplace, you can expect them to take more chances on out-of-the-box thinking and creativity, not to mention increased productivity.

But you can't expect your employees to feel safe expressing their identities, and thus their ideas, if you don't first create an inclusive environment for them. But how do you create a space in which your team feels safe drawing from their unique perspectives?

One way to make your employees feel more visible and heard is through diversity networks, groups that come together based on shared identities, like single moms, veterans, LGBTQ individuals, Asian-Americans, the disabled or Latinx. These networks help individuals support and learn from one another, share resources and discuss the challenges and stereotypes facing this facet of their identity and how to address them. If you're worried that this could divide the office more than unite it, don't be. These networks empower individuals to share their experiences with the broader team, allowing everyone to learn from each other.

You also need to make sure you allow opportunities for team members to express themselves. The quickest way to make an employee feel uncomfortable and unaccepted is to have their co-workers interrupt or speak over them. Provide moments for individuals to talk about the projects they are working on, their goals and their struggles.

Diversity training can be helpful in the office. The fact is, everyone has a bias, and it's usually subconscious. Diversity workshops can be a great way to unpack our biases and privilege. Being able to listen and empathize is a vital skill in any business setting, and will improve not only communication between your employees, but their customer service skills as well. A diversity workshop should not be a lecture, but rather an opportunity for honest conversation and learning.

Institute an open-door policy so that your employees feel safe coming to you and their other bosses about issues of discrimination, sexism, racism, homophobia and more. First and foremost, listen. Don't invalidate their experiences by immediately questioning them or taking a side in the conflict. This, plus literally keeping your door open as often as possible, will instill a feeling of trust in your office.

Show that diversity is important to you by hiring employees who come from a variety of backgrounds. Your work team should ideally represent the full diversity of your customer base, enabling them to relate and appeal to your clients on a personal level. Representation also works as a strong motivator. When individuals can see themselves in their role models — bosses, podcast guests, interviewees, etc. — they'll be more likely to imagine higher goals for themselves.

MIKE MICHALOWICZ started his first business at the age of 24, moving his young family to the only safe place he could afford-a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small business columnist for The Wall Street Journal; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book The Toilet Paper Entrepreneur. His newest book, The Pumpkin Plan, has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com/

Who Else Wants To Win A $250 Gift Card

The Grand Prize Winner of last month's Trivia Challenge Quiz is Debbie Green from DDC Engineers! Debbie's name was randomly chosen among those that correctly answered my quiz question from last month: **Which of these events occurred FIRST: the computer chip was patented, the Berlin Wall was erected, the birth control pill was OK'd by the US Food and Drug Administration?**

The answer was a) Computer chip patented. Now, for October's trivia question:

When was the first "Peanuts" comic strip written by Charles Schulz published?
a) October 9, 1949 b) October 2, 1950 c) October 21, 1951 d) October 4, 1952

Email bhinson@creativeconsultants.net with your answer!

Yahoo's 3 Billion Breached Accounts Are a Boon to Identity Thieves

Calling the exposure of a whopping three billion Yahoo accounts a mere "hack" undermines the magnitude of the breach, and it does a disservice to the sheer damage that has occurred and could still come from what is a truly monumental cybersecurity failure.

Yahoo wasn't just hacked back in 2013 — the company's three` billion user accounts were completely exposed, resulting in a massive treasure trove for criminals, looking to profit from the sensitive information.

Much of the information stolen is used to identify customers online. And given common unsafe password practices, it means ripple effects with even more compromised accounts and exposed personal data could continue.

To put the sheer scale of the breach in perspective, if all three billion Yahoo accounts were unique individuals, it would represent 40 percent of the world's population. Of course, it's likely that many users had multiple accounts with Yahoo. Even still, every single one of those accounts had their passwords and personal information exposed. No Yahoo customer was safe.

What's worse, while the hack occurred in 2013, but wasn't disclosed until December of 2016, meaning potentially billions of individuals were vulnerable without their knowledge. Even the scope of it wasn't fully understood until this week, when Yahoo's new parent corporation Verizon revealed that all accounts owned by the internet giant were affected.

Yahoo's security failure is just the latest in a string of unprecedented data breaches, including recent incidents at Equifax and Deloitte. But the Yahoo breach is unique because it is a global incident that potentially affects a majority of users within the connected world. At one point, almost everyone on the internet had a Yahoo account.

The "hack" once again spotlights the need for better identification methods and security practices, particularly for companies that handle online transactions and sensitive data.

As these security failures continue to mount, cybercriminals will cross-reference growing, extensive databases of stolen information to target victims and successfully take advantage of them. Theft, fraud, phishing and more are all likely to grow as bad actors become more knowledgeable and powerful.

In response, individuals can be more protective of the kinds of information they are willing to share online and with corporations. Does Facebook really need to know every town you have lived in? Users should also begin adopting better password practices to ensure that one account breach does not potentially endanger their entire online presence.

Consumers need to fight back, but they're going to need help somewhere along the way. Businesses also need to invest in security in a meaningful way to prevent attacks, while also investigating new and alternative ways of identifying customers.

It's clear that the current systems of identity — email addresses, credit cards, and Social Security numbers — are failing us. This year alone there have been more than 20 high-profile breaches. These unprecedented failures are the wake-up call the world desperately needed. How we respond will help decide just how much precendent the next "hack" will carry.

--Travis Jarae, *The Hill*