The Tech chronicle

Billions Breached

This is becoming so common place that it doesn't seem to be a big deal to most now.

More and more companies are breached, more and more client's personal information is being sold on the dark web.

Are you keeping an eye on your dark web presence? Do you even know how to do so?

Are you one of the 15 billion credentials on the dark web?

Read the article in our July 20, 2020 blog.

Why NOT Investing In IT Can Cost You BIG

If you haven't invested in IT security, then your business is at risk.

These days, it's easy to take technology for granted. It just seems like everything works so well. If things are working well, why spend more on things like data monitoring or secure cloud storage?

Here's a startling fact: a lot of business owners take this approach to network security. They might think, "This will never happen to me," when it comes to data breaches, malware and hacker attacks. While they might be great at running their businesses, they may end up skimping on their IT security.

They see it as something they simply don't need to invest in. But a lot of business owners end up paying big because they aren't serious enough about IT security. A simple virus scan app or firewall just isn't enough. Hackers and cybercriminals are *relentless*.

Here's another startling fact: threats like data breaches, malware and hacker attacks are a lot closer than you think. When you go cheap with your network security or don't work with an experienced IT services company, it can end up costing you big in the long run.

A lot of business owners skip out on things like network security, cloud backup, data protection and data monitoring because they don't like the up-front cost or another monthly bill. In reality, while you can expect an ongoing cost, working with a managed IT services firm can be

Continued on pg.2

August 2020

This monthly publication provided courtesy of Carlos Soto. Franchise owner since 2005.

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.

Continued from pg.1

remarkably cost-effective (and smart!).

When your network security solutions are running smoothly, you won't know it. It all happens in the background. But because it's not something you "see" on a daily basis, you might wonder if you're really getting your money's worth. This can be a challenge for business owners who may want to see tangible results for something they pay for. The good news is that you *can* get tangible results!

Many IT services firms let businesses customize their reporting. You can actually get daily, weekly or monthly reports from your IT security company! You can see exactly what they're doing for your business and the exact threats they're protecting you from.

More than that, a good IT services company is going to work closely with you. They'll provide you with the information, resources and tools you need in order to focus on your customers and the successes of your business. They'll educate you and your team and help you identify the best technology for your needs. That's the definition of peace of mind!

Here's why it can be so costly to NOT invest in IT security:

SCENARIO 1: Imagine you're hit with a malware attack, and it takes your network out of commission. Customer data is at risk, and your business comes to a screeching halt. You have to call in IT experts to fix the problem ASAP. This is a break-fix approach to IT services.

> **"When your network security solutions are running smoothly, you won't know it."**

In this event, you're going to be charged BIG to get your business up and running again. The IT specialists will have to scrub your network and make sure everything can be recovered. Not only do you have to pay to get your network cleaned, but your cash flow also takes a hit while you wait around to get everything fixed.

SCENARIO 2: You're hit by a data breach. Hackers are looking for information they can exploit, such as credit card numbers, passwords and other identifying information. They often sell this information to other cybercriminals. In almost every case, this information CANNOT be recovered. Once it's gone, it's gone.

This means you have to take action FAST to make sure stolen information cannot be used. This includes changing credit card information and updating passwords. In the event of a data breach, the sooner you inform your customers, the better. But this is a double-edged sword. Your customers need to know so they can protect themselves. At the same time, your customers may lose faith in you because you put their data at risk.

These are just two examples out of many. When you don't take IT security seriously or you're cheap with your technology, it can end up costing you BIG in the end. Work with an IT security company that will work with you to protect your business the right way – and help you avoid scenarios just like these.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
go.ctmaryland.com/protect
or call our office at (240) 399-9600.

New Services

Threats are nothing new, nothing surprising, nothing shocking (almost) anymore.

Every day there are new ways we are under attack for information. Information that can be taken away and exploited for others to gain from.

How hard is it to protect your systems? It's a never ending answer because today's solutions will not work for tomorrow's problems. Tomorrow will bring a new set of issues that will require a new set of resolutions.

We have been playing this game since what seems like forever. The game pieces change but the rules remain the same. Protect those who can't protect themselves. Arm those so that they can be protected.

We continually grow in knowledge and exercise that knowledge and develop and work with new services to serve and protect our clients.

We have added new, refined and expanded our current service offering for our clients.

We are implementing this knowledge and continue fighting for the safety of our client's systems. The fight continues.

It Better Be Packaged Right

Joshua Bell is a world-renowned American violinist who made his Carnegie Hall debut at the age of 17 and now performs with the world's premier orchestras and conductors. His talent causes concertgoers to flock to the greatest concert halls in the world where the average seat costs $100 and front-row seats are in the thousands.

The *Washington Post* newspaper set up an impromptu concert with Bell as an experiment on perception and priorities. Would people in a hurry recognize the brilliance of this musician, even though he was dressed in jeans, a long-sleeved T-shirt and a baseball cap? Would the beauty of his music transcend the moment and cause them to pause and enjoy this incredible talent in the busy train station in Washington, DC? Would priorities take precedence over listening to an international virtuoso who had recently won the Avery Fisher Prize as the best classical musician in America?

The only thing that was exceptional to see for those who passed by Bell that day was the $3.5 million Stradivarius violin he was playing (made in 1713). But to those who saw him playing, it just looked like a regular old violin. The "package," the perception of the concert, didn't draw people's attention, even though the talent was exceptional. There was no advertising, no fanfare, no hype, no fancy clothes, no amazing concert hall or fabulous stage – it was just some guy in a baseball cap, standing up against a wall with his violin case open to receive donations.

Could a man who is paid $1,000 per minute to perform, a man who was playing the music of Bach, Brahms, Ponce and Massenet, get their attention? Not really. The three-minute video will show you that 1,097 people passed by. Only 27 people put money in his violin case as they walked by, and of those 27, only seven of them paused for a moment to listen. Bell made $32.17 in 43 minutes of playing. There was NO applause or acknowledgement of his skill … a skill that, three days prior to this experiment, had drawn people to completely fill Boston's Symphony Hall.

See Bell playing at the Metro at YouTube.com/watch?v=LZeSZFYCNRw.

The point I am trying to make is that packaging is critical. When you are making a presentation to your client, boss or peers, you can never forget that. You may have all the data and skills to make the presentation, but if you want to stand out, then pay attention to how it is packaged. Perception isn't everything, but it helps. As the experiment with Bell proves, it takes a lot more than just talent to get their attention.

Author Terry Goodkind once said, "*Reality is irrelevant; perception is everything.*" If a person doesn't perceive the value, then to them, it's not valuable. Good packaging

Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys *and* 52 Essential Habits For Success, *he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Tony Robbins, Tom Peters and Stephen Covey. Today, he travels the world, sharing powerful ideas for achieving*

Don't Overlook This 1 HUGE Issue In Your Company

Is it possible to communicate too much? Yes! In a report from GuideSpark, researchers found that the average employee receives about nine e-mails every day that are labeled as "must-read," which means these e-mails are relevant to their day. These are mixed in with less relevant e-mails, and that causes a lot of clutter.

This is just one form of communication we deal with every day. Add in face-to-face, phone and text communication, and it really piles up. It becomes a communication overload.

Communication overload destroys productivity. E-mails take time to read and to respond to. When your in-box becomes full, you're looking at a large part of the day.

How do you fix this? Prioritize your messages. Use e-mail as efficiently as possible and keep it short. Avoid sending company-wide e-mails if they aren't relevant to everyone. Target e-mails to the people who need that information. Also, if employees are getting outside e-mails that have zero relevancy, unsubscribe from those sources. *Small Business Trends, May 12, 2020*

Staying Secure In A Social Media World

The age of social media has let millions of people reconnect and stay up-to-date with family members, friends, in-laws and acquaintances. It also continues to shape how we all communicate with each other. It's important to keep a few things in mind before you check your newsfeed.

There is no delete button on the Internet. Everyone knows how to capture a screenshot. Even if you keep your social media completely private, when relationships change, nothing is private. Are you going to be comfortable in 10 years with what you post today? It will be archived forever. If you post in online forums or comment on news-related websites, consider using a pseudonym. Don't share names of real businesses, clients, friends or family. If a bank manager wouldn't allow a picture of all of the money in the vault to be shared on the Internet, then you shouldn't allow a picture containing any confidential, financial, legal or other protected documents and items to be shared either.

A good social media policy in the office now can save headaches down the road.

Top Tips For Improving Remote Working

Limit meetings. Remote meetings over Zoom, for example, can bring productivity to a halt. While in-office meetings also slow productivity, Jason Fried, CEO and founder of Basecamp, suggests it's more harmful in a remote setting. Instead, focus communication through simple e-mails or chat apps.

Foster community. Leaders within your company should routinely check in on the rest of the team. Ask them how their work is going, how their weekend was or what they're looking forward to in the week ahead. A little regular social interaction goes a long way.

Have a dedicated workspace. The great thing about remote work is that you can do it anywhere. But this can also invite distraction. Encourage your team to have a dedicated work environment outside of their normal living space. Having access to a door that can close is invaluable! *Inc., May 7, 2020*

Proactive Protection

Computer Troubleshooters
TECHNOLOGY SOLVED

FIGHT BACK

It seems like every week another major corporation announces a large-scale security breach. For IT Managers, it's a concern that is requiring an increasing amount of time—and it's not a problem that is limited to Fortune 500 companies.

In the past, cyber attackers typically targeted a single large organization with the hopes of landing one significant payout. Today, hackers are more strategic. They distribute their efforts, targeting a number of smaller firms in order to yield multiple smaller payouts—and it's a system that is working. So what do you do about it? Easy. You take the fight to them.

Hunt Hackers Down

Traditional enterprise security products focus on keeping hackers out. But what happens when someone breaks through? In today's ever-changing threat landscape, security experts are encouraging organizations to assume that a compromise has already taken place. That's where Huntress comes in. Developed by ex-NSA hackers, our Managed Detection and Response service augments your existing security stack by proactively seeking out potential footholds and persistence methods.

The process is simple. First, our lightweight endpoint agent will gather data and submit it to our cloud for analysis. From there, our highly skilled team and algorithms will review the data to identify any potential threats. If a breach is detected, we'll provide your IT Staff with an actionable report, along with step-by-step instructions to remediate the threat.

The best part? Your team won't need any specialized (and costly) training.

Why Detection & Response

Operated by Operators
Our threat operations team is comprised of former penetration testers and reverse engineers with over a decade of advanced forensic security experience.

Plays Well With Others
Our active threat hunting system works seamlessly with your current security stack.

We Do The Heavy Lifting
Our algorithms and experts actively hunt for hackers, identifying and reporting their footholds and persistence methods.

Turnkey Remediation
When a threat is detected, you'll receive step-by-step instructions that tell you how to eliminate it once and for all.

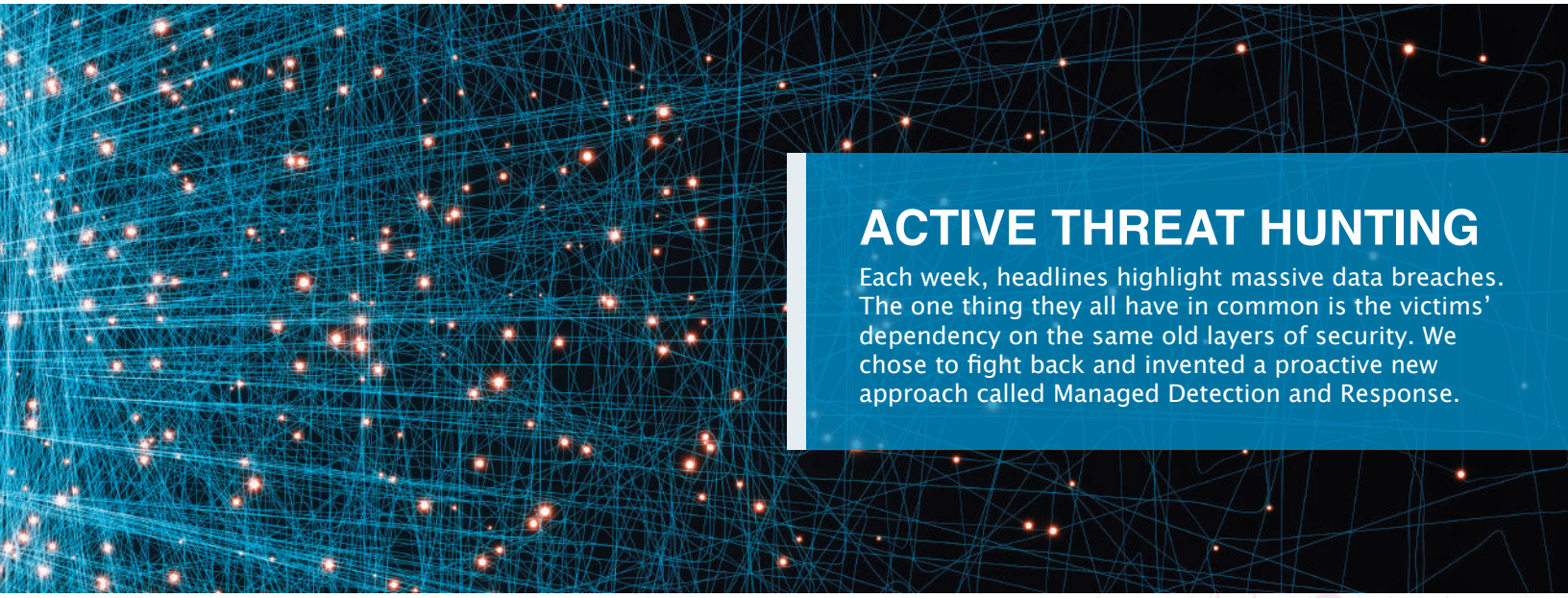
Deploy in Minutes
Our partners have deployed Huntress to THOUSANDS of clients in less than 10 minutes using their existing RMM software.

Learn more at www.ctmaryland.com

HUNTRESS

A New Approach

Computer Troubleshooters
TECHNOLOGY SOLVED



ACTIVE THREAT HUNTING

Each week, headlines highlight massive data breaches. The one thing they all have in common is the victims' dependency on the same old layers of security. We chose to fight back and invented a proactive new approach called Managed Detection and Response.

Why Does it Work?

Modern antivirus programs primarily detect malicious applications and behaviors using patterns, called heuristics and signatures, to identify known viruses. But in a threat landscape that is constantly evolving, does this strategy really work? It does…to a point. This is where Managed Detection and Response comes in.

Our industry-leading threat hunting solution complements your existing security stack to identify new and old footholds missed by antivirus, regardless of how your computers were compromised.

> **ADVANTAGE:**
> Huntress makes hackers earn every inch of their access within the networks we protect.

How Does it Work?

COLLECTION

1

Our endpoint agent collects a new type of indicator called "persistence mechanisms" from desktops, laptops, and servers. This data is then sent to our cloud-based analysis engine for deep inspection. Worried about productivity or data privacy? Don't be.

The agent's lightweight design ensures your users won't even notice that Huntress is constantly monitoring. As for your data, it's all encrypted—in transit and at rest.

ANALYSIS

2

Once we receive the data, our analysis engine and threat operations team uses file reputation, frequency analysis, and machine learning to quickly hunt and investigate suspicious footholds.

When a threat is detected, Huntress delivers more than an alert. Your IT Staff receives step-by-step recommendations to prioritize the threat, remediate the incident, and address the root cause.

Learn more at www.ctmaryland.com

HUNTRESS