The Tech chronicle

Ransomware Death

Woman dies during a ransomware attack on German hospital.
This could be the first death directly linked to a cybersecurity attack.
She could not be attended so she was sent to another facility twenty miles away.
And this attack was really meant for a nearby university and not the hospital itself.
Sad to hear news like this but it brings to light that ransomware can hit anyone at anytime. You need to take precautions before it's too late.
https://www.theverge.com/2020/9/17/21443851/

October 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.

The #1 Mistake Your Employees Are Making Today That Lets Cybercriminals Into Your Network

We all make mistakes. It's a fact of life. But as we all know, some mistakes can have serious and lasting consequences – especially when it comes to business, cyber security and the constant cyberthreats that are out there.

While some businesses have invested heavily in cyber security, many have not. When it comes to network and data security, one of the most vulnerable areas of the economy is small businesses.

More often than not, small businesses simply don't go all-in when it comes to IT security. Some fear they don't have the budget and worry that IT security is too expensive. Others don't take it seriously – they have an "it will never happen to me" attitude. Then there are those who invest in *some* security, but it's limited and still leaves them vulnerable in the long run.

But there is one area of IT security where *every* business is vulnerable. You can have the greatest malware protection in the world and still fall victim due to this one big mistake.

Your employees lack IT security training.

It's as simple as that. When your team isn't trained on IT or network security *and* they aren't aware of today's best practices, you open yourself to major risk. Here's why: We make mistakes.

Scammers and cybercriminals have the most success when they are able to trick people or play on the emotions of their victims. One common emotion they use is fear.

No one likes to get a message telling them that their bank account has been compromised. This is how phishing e-

Continued on pg.2

Continued from pg.1

mails work. The scammer sends an e-mail disguised as a message from a bank or financial institution. They may tell your employee that their account has been hacked or their password needs to be changed immediately. They use fear to trick them into clicking the link in the e-mail.

So, concerned about their bank account, your employee clicks the link. It takes them to a web page where they can enter their username, password and other credentials. Sometimes it even asks for their full Social Security number. (Scammers are bold, but people fall for it!)

As you guessed, the web page is fake. The link in the e-mail directs your employee to a page that allows the scammer to collect their data. Some thieves use it to access their bank account, but others sell the information for a quick buck. No matter the situation, the information has fallen into the hands of crooks.

The challenge is that phishing e-mails have gotten harder to spot. Scammers can spoof legitimate web addresses. They can make fake e-mails look like the real deal. But there are still plenty of minor details that indicate the e-mail is a fake.

This is one of the MANY reasons why comprehensive employee IT training is so important. Training helps employees identify red flags. But more than that, it helps them identify *changing* red flags. For instance, a phishing e-mail from 2010 looks nothing like a phishing e-mail from 2020.

"Your employees are your first defense against outside cyber-attackers."

Scammers stay ahead of the curve. They know the trends, and they know how to adapt. Your employees also need to know the trends and need to be ready to adapt.

Good IT training covers much more than phishing e-mails. It helps your employees identify security red flags across the board.

These include:

- Phishing e-mails and phone calls
- Poor or outdated passwords
- Malicious software hidden in links, attachments or online ads
- Poorly configured security on employee devices (a big deal for remote employees!)
- Lack of guidelines related to Internet or social media usage on employee devices
- Outdated software or hardware

Good training is also continuous. Cyber security training isn't a one-and-done deal. It's something you do every quarter or twice a year. Just as you keep your business's equipment maintained, you have to keep your employees' cyber security knowledge maintained. After all, your employees are your first defense against outside cyber-attackers. When they know what they're dealing with, they're better equipped to stop it in its tracks and protect your business.

The bottom line is that a lack of training is the biggest threat against your computer network and the health of your business. You need to have a strong training program in place to make sure your employees stay up-to-date. But you don't have to do it yourself. We can help. Along with your team, let's protect your business together.

Free Report Download: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This…

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

Get your FREE copy today:
go.ctmaryland.com/cloudreport

Are You Protected

Keeping your systems protected is the first line of defense.

1. RMM
2. Account management
3. Privatise
4. Document management
5. ID Theft Protection
6. Backup
7. Ransomware Protection
8. Huntress
9. Dark Web Monitoring
10. HelpDesk Services
11. Exchange Office
12. Secure FileSync
13. Managed Firewall
14. HaaS
15. VoIP
16. Virtual Computing
17. Disaster Recovery

We have a host of services that you should be implementing to keep you systems as well as your network secure and protected. The design is to keep you up and working with the ease of knowing that your systems will function securely when you need them. How do you rate?

What Makes A Leader Successful Today?

Intentionality And The 3 Shifts

Have you ever wondered what one thing all successful leaders have in common? First, consider what all *unsuccessful leaders* have in common: they lack focus.

Either they aren't clear on what they're trying to do or they know what they need to do but aren't doing the right things to achieve their objectives. Both waste money and resources and leave organizations stuck in the status quo.

This affects leaders regardless of the size or type of organization, and that's why I wrote *The Intention Imperative: 3 Essential Changes That Will Make You A Successful Leader Today.*

What all great leaders have in common is intentionality— *being crystal clear on what you're trying to achieve and taking the right actions every day to achieve it.*

Why do many business leaders lack clarity?

1. They inherited an unclear vision or never had one to begin with.
2. They value operations over objectives — doing things without questioning why.
3. They were distracted by problems, or even opportunities, which took them off course.
4. They were unwilling or unable to look at what was consistently being done with a fresh perspective.

What are the symptoms and signs of a leader who lacks clarity?

1. Constant changes in focus or direction
2. Lack of momentum
3. Confusion among employees and what to do
4. Many team members asking "Why?"
5. Frustration at every level
6. Inconsistent action or behavior

In my book, I explain intentionality and then share what I believe are imperative changes leaders need to take today to succeed: the shift from *structure to culture*, from *motivation to inspiration* and from *experience to emotion*.

IMPERATIVE 1 – CULTURE
"Culture is what we think and believe, which then determines what we do and what we accomplish."

In *The Intention Imperative*, I teach the five levers you have for creating and maintaining the culture you desire. Creating it is the job of a leader.

IMPERATIVE 2 – INSPIRATION
"Inspiration doesn't have to be mysterious or complicated to create."

What is inspiration? It is motivation to the power of purpose. It is linking meaning to motives. Inspiration doesn't come from outside force or artificial causes. It develops from the work itself and how the leader is able to demonstrate importance and impact.

IMPERATIVE 3 – EMOTION
"Emotions are everywhere and they are the single biggest factor in how we make decisions."

A negative emotional experience can be offset with a positive one. The customer experience is important, but how the customer feels about that experience is critical. Few companies design and deliver for positive emotion.

Now, try these three things:

1. Focus on building a culture that powers the right actions to create the right results you, your team and customers need for breakthrough success.
2. Couple purpose with motivation so your team is inspired.
3. Design your product and service delivery around positive emotions.

Mark Sanborn, CSP, CPAE, is the president of Sanborn & Associates, Inc., an "idea studio" that seeks to motivate and develop leaders in and outside of business. He's the best-selling author of books like Fred Factor *and* The Potential Principle *and a noted expert on leadership, team building, customer service and company change. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out any of his excellent books, his video series "Team Building: How To Motivate And Manage People" or his website, MarkSanborn.com, to learn more.*

Improve Your Cash Flow With These Tips

Have Better Billing Processes – Make it as easy as possible for customers to pay their bills. Incentivize them to pay before the due date with a small discount or offer. Be diligent about sending invoices ASAP after customers buy with you.

Get Cooperative – If it's possible or practical, work with other businesses to form a buyers' co-op. This gives you more buying power when buying in bulk.

Credit Check Customers – When dealing with higher-priced goods or services and a customer can't pay in cash, don't be afraid to run a credit check. Customers with poor credit can be a liability and cost you big.

Audit Your Inventory – Identify what costs you money by sitting around. If you're stuck with inventory that isn't moving, you may need to discount it to get rid of it.

Pay Online – Pay all of your bills online. This way you can select the exact date when those bills are paid each month, giving you more control over your cash flow.
SmallBiz Technology, Jan. 27, 2020

Top Ways To Prevent Your Remote Workers From Letting Cybercriminals Steal Your Data

1. Set expectations, rules and boundaries for employees, ensuring everyone is on the same page and held accountable.

2. Put together standard operating procedures for employees so they know what to do and who to call should anything go wrong.

3. Have a disaster recovery plan ready to back up and restore any system or data, should it become compromised.

4. Establish guidelines for employees, defining which approved devices and software they should be using.

5. Make sure those devices and software are routinely updated with the latest security patches.
Cyber Defense Magazine, June 3, 2020

3 Things You Can Do To Use Stress To Your Advantage

Embrace Deadlines – Research suggests we are the most productive with deadlines looming. Give yourself deadlines for everything. If you struggle with procrastination, move deadlines up in order to get things done.

Stress Yourself Out (On Purpose) – You can actually build a tolerance to stress. All you have to do is step out of your comfort zone and intentionally put yourself into stressful situations. You become more resilient to stressful situations and test your own boundaries at the same time.

Identify Stress "Weaknesses" – When stressed, identify what it is about a situation or task that is causing you stress. Then, focus on that cause and determine what you can do to mitigate it. It might mean reorganizing your day, such as reading and responding to e-mails at a different time. Or maybe you need more information on the issue you're dealing with, so do some research and see what you can find to help.
Inc., July 8, 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.

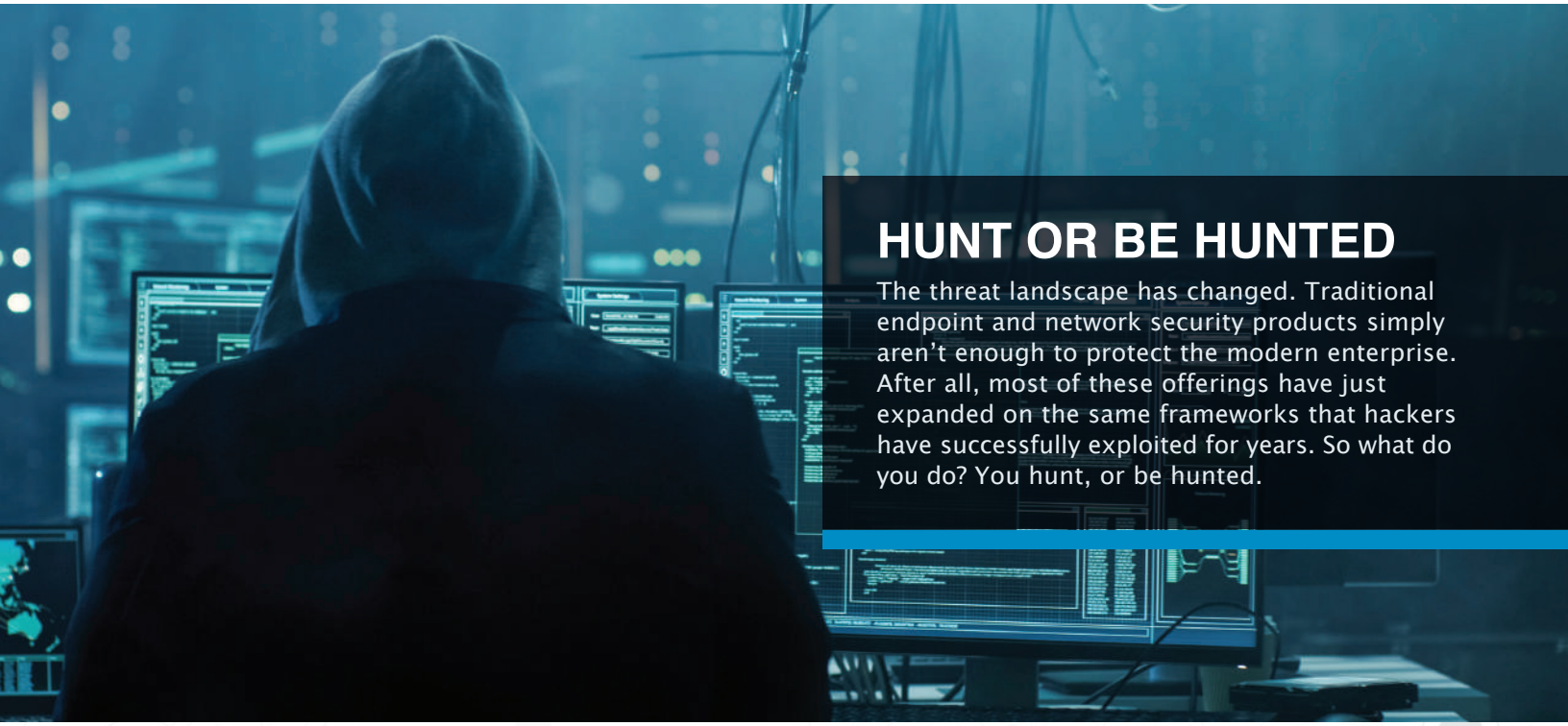
Deploy in Minutes
Our partners have deployed Huntress to THOUSANDS of clients in less than 10 minutes using their existing RMM software.

Learn more at www.ctmaryland.com

HUNTRESS

Breach Detection

Computer Troubleshooters
TECHNOLOGY SOLVED



HUNT OR BE HUNTED

The threat landscape has changed. Traditional endpoint and network security products simply aren't enough to protect the modern enterprise. After all, most of these offerings have just expanded on the same frameworks that hackers have successfully exploited for years. So what do you do? You hunt, or be hunted.

A Different Way

In a security environment that is ever changing, the best way to stay on top of potential threats is to start throwing punches. Huntress Labs' "collect-and-analyze" approach to active threat detection makes hackers earn every inch of their access. Working in tandem, our proprietary endpoint agent and U.S. based threat operations team significantly reduces the time to detection, allowing you to destroy malicious footholds as soon as they are created. It's an unbeatable combination: machine learning and tenured forensic security experts.

You Can't Afford Business as Usual

$11.7 MILLION
– the average estimated cost of cyber attacks to global firms per year[1]

$5 BILLION
– the estimated total damages of ransomware globally in 2017[2]

60%
– the portion of SMBs that took 30+ days to recover from a hack[3]

3X
– the rate at which the cyber crime epidemic will necessitate new IT security positions[4]

1 https://www.securitymagazine.com/articles/88338-cyber-crime-costs-117-million-per-business-annually
2 https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html
3 https://www.darkreading.com/endpoint/most-small-businesses-lack-response-plan-for-hacks/d/d-id/1327181
4 https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html

Learn more at www.ctmaryland.com

HUNTRESS

Layered Security

Computer Troubleshooters
TECHNOLOGY SOLVED

DEFENSE REIMAGINED

There's no getting around it: cyber attackers are growing increasingly sophisticated in their tactics. From web apps and operating systems to hardware and human error, today's hackers leave no potential vulnerability unchecked. But that's why you have antivirus, right? Not so fast.

If recent headlines have taught us anything, it's this: A determined hacker can bypass even the most robust security program. So what should an organization do? The answer is simple: layer your defenses to address the gaps in your strategy.

Defense in Depth

Developed by former NSA cyberwarfare operators, our managed detection and response service represents a new layer in the security stack. Combining automated collection tools with expert analysis, our team actively hunts down threats that may have slipped past other layers of protection. On a daily basis, this new approach uncovers hackers abusing trusted applications and built-in Windows features to evade defenses for months.

Designed to complement your existing security strategy, Huntress analyzes the overlooked methods attackers use to persist within your network. Our managed detection and response service allows you to address these gaps, stopping advanced threats and cutting-edge malware in their tracks. This defense-in-depth model reduces time to detection and provides more comprehensive protection for your organization's IT assets.

Are You Covered?

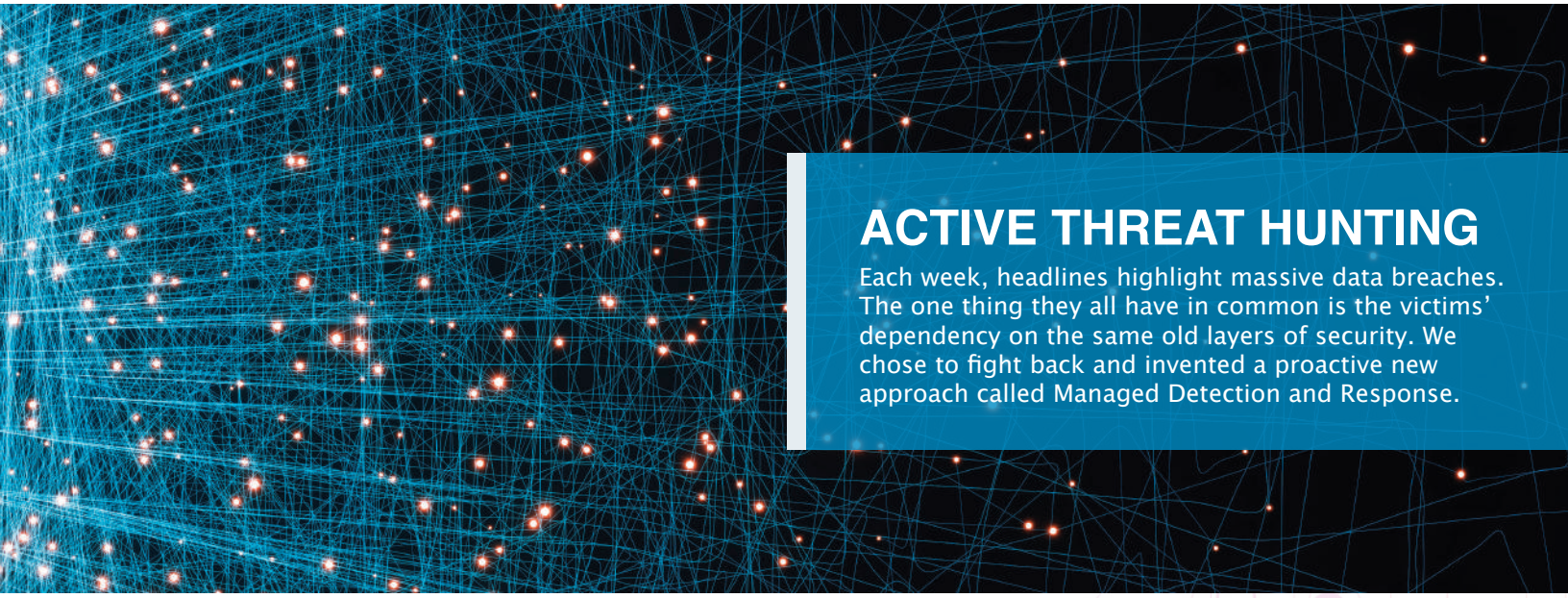
	Antivirus	Huntress
Monitors Application Behavior	—	
Protects Users Without Interruptions	—	—
Prevents Known Malicious Threats	—	
Minimizes Risk of Downtime & Data Loss	—	—
Proactively Hunts Anomalous Threats		—
Triages Events with Human Analysts		—
Prioritizes Alerts with Business Context		—
Delivers Resilience & Remediation Guidance		—

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