The Tech chronicle

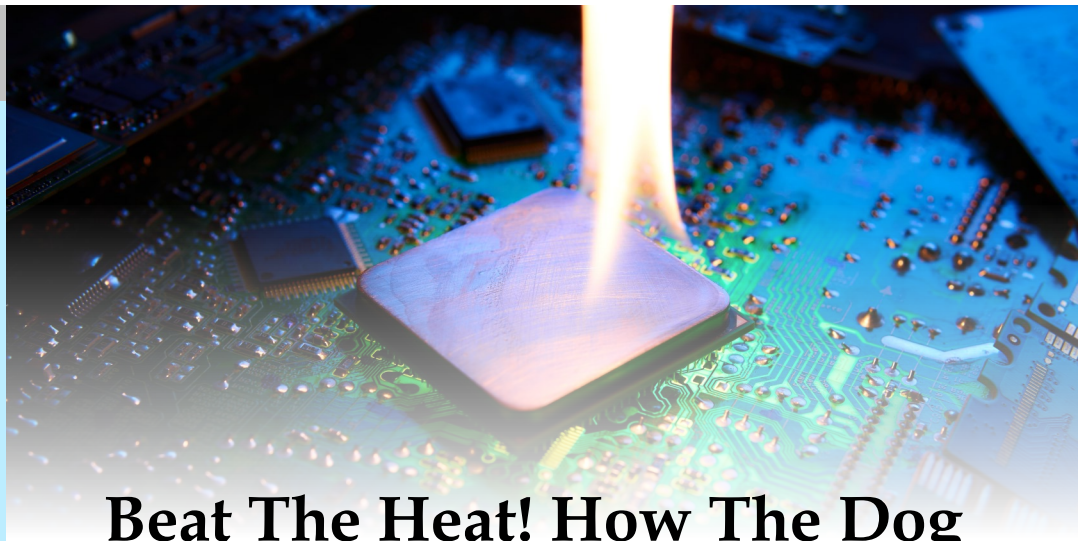
Who's Next?

Morgan Stanley Banking is the latest to get hit by a data breach.
Another day, another hack. Hacks continue to evolve as the hackers get more and more sophisticated.
Morgan Stanley's network was breached after an attacker stole personal information belonging to their customers by hacking into a third-party vendor, then using that information to hack into Morgan Stanley's network.
Crazy right? Be on the lookout for a letter from MS if you are affected. Read more about it on our July 23rd blog.

August 2021

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.



Beat The Heat! How The Dog Days Of Summer Can Wreak Havoc On Your Technology

The dog days of summer are here, and it's hot out! Homeowners and business owners alike are bracing for their upcoming power bills as they run their air conditioners around the clock trying to keep cool. But for many business owners, it's not just about keeping your team cool – it's also about keeping your technology cool.

Every piece of technology you use is susceptible to heat damage. Sometimes they overheat due to internal issues. Maybe they're processing a lot of data. Or maybe the internal cooling system isn't enough. But they can also overheat due to external issues, such as high summer temperatures and inadequate air conditioning.

If heat overwhelms your systems, it has the potential to knock out your business. If computers go down or servers can't run efficiently due to heat, it can be a costly disaster. The average computer is built to work in external temperatures of 50 to 82 degrees Fahrenheit. Laptops and tablets can handle 50 to 95 degrees Fahrenheit.

Every business should be aware of just how much damage heat can cause. For example, heat can damage individual components in your devices. There are records of graphic cards bursting into flame as a result of overheating and heat-related electrical issues. These components are designed to withstand high heat, but they can only take so much.

Heat can also disrupt productivity. It's one thing if your business is warmer than usual and you have fans running. It can make work

Continued on pg.2

Continued from pg.1

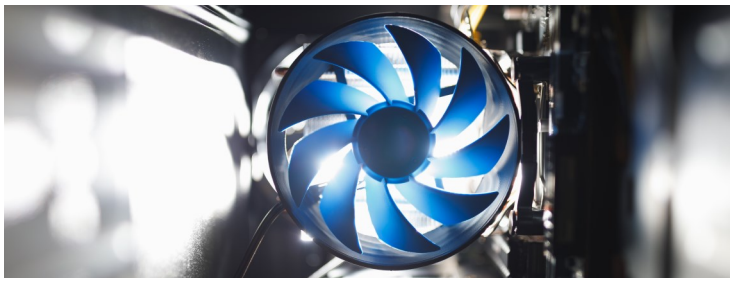
harder. But heat slows down devices. They cannot run as efficiently and, as a result, programs and apps will struggle to run. In some cases, they might not be able to run at all because they require a certain amount of data processing that is negatively impacted by too much heat.

If your systems are disrupted or damaged, you can also lose critical data. Heat can damage hard drives and solid-state disk drives, leaving you without access to your data. Sometimes, with proper cooling, this data can be recovered, but if the heat and damage persist, the data may be unrecoverable if you don't have a backup.

What's the next step? Every business needs to fully understand its cooling needs. It's one thing to cool people working in an office. It's something else entirely to cool a server room. Ask yourself questions like:

- Does your business have adequate and efficient air conditioning?
- Does your technology (such as a computer or server room) have adequate air conditioning?

> **"Every piece of technology you use is susceptible to heat damage."**



- Do individual devices have adequate cooling (have employees complained about weird app slowdowns)?

On top of this, it's critical to ask questions about your data security needs:

- Do you keep all of your data on-site?
- Is your data protected from natural disaster or outside intrusion (have you invested in cyber security)?
- Do you have a plan if your data is damaged or lost?
- Do you routinely back up your data to the cloud or another off-site solution?

You never have to compromise your data or your business. There are countless solutions on the market today to help you protect your most valuable assets – and to help with your technology cooling needs. As you navigate the dog days of summer, remember you have options. A managed services provider (MSP) or an experienced IT services firm can help you determine if your tech is as cool as it should be. They can help you ensure the longevity of your technology and keep your data safe.

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 send and email to info@ctmaryland.com

PrintNightmare

Have you heard of this? PrintNightmare is a critical security vulnerability affecting the Microsoft Windows operating system. The vulnerability occurs within the print spooler service. There are two variants, one permitting remote code execution, and the other leading to privilege escalation.

No matter how you look at it, it is a bad thing if you get hacked via this vulnerability. The solution is easy, just disable the print spooler. The drawback is that you will no longer be able to print. Not a real solution.

Microsoft has released a patch to help with this issue. After scrambling and getting systems patched, security researcher Will Dormann reported that he had found a way to bypass the new restrictions the new patches put in place. This may not be the end of the issue. It is, nonetheless, a big step forward and a clear sign that the PrintNightmare will soon be ending. But not soon enough.

Getting your system patched is more important than ever because systems that never get properly patched, are the highest point of attack. Knowing that there is a security hole, provides a "how-to" hack into a system. Read more about this vulnerability in July 22nd blog post on our website .

Break The Bottleneck

The X-Factor For Exponential Advantage

Breaking the bottleneck starts with asking the right questions. Innovators ask what *could be*, not what *is*. They ask, "How can I find greater potential from every person, situation, process, experience and outcome?"

Before you even start the process, you have to understand the difference between execution vs. innovation. If you focus only on execution, you won't get exponential leverage. Carve out a small amount of time for innovative thinking and you will scale the company. For instance, your planning sessions – whether they're weekly, monthly, quarterly, etc. – should break down this way:

- 90% on execution
- 10% on innovative thinking

One area we encourage people to really think about is industry bottlenecks. What are five industry bottlenecks you face (including your top three competitors)? We like to break it down into five diagnostic levers:

- Eliminating expense
- Customer buying or usage experience
- Customers' psychological barriers
- Winning hearts and minds
- Eliminating negative externalities

For example, when it comes to eliminating expenses, you can look at your top five costs or how those costs relate to your revenue. Your main expense may be labor or, getting more specific, revenue per employee. Of course, you don't want to just eliminate labor – you want to look at ways to increase productivity.

What is getting in the way of customers buying or using your products or services when or how they want to? Write down five industry bottlenecks related to that. Jumping into customers'

psychological barriers, why might they be embarrassed or unsure about using your products or services? What are five psychological bottlenecks in your industry?

We also look at the hearts and minds. What can you do to win the hearts and minds of a key constituency group that would really propel your company to growth? It doesn't just mean winning the hearts and minds of customers, but those of your workers. Consider Chick-fil-A vs. McDonald's. Chick-fil-A delivers a high level of service because their workforce is happy. Their profit per square foot basis is more than that of McDonald's, and they're only open six days a week.

Lastly, in eliminating negative externalities, look at the "harm" your business may do to things like your community or environment. What can you do to mitigate these things? This isn't always an easy one to figure out or answer – and there might not even be anything. But look for things that have the potential to do harm, whether it is your community, customers or even the business itself.

P.S. See the full Petra Coach webinar for *Break The Bottleneck: The X-Factor For Exponential Advantage* at **PetraCoach.com/break-the-bottleneck-the-x-factor-for-exponential-advantage-with-barrett-ersek**.

Barrett Ersek is a serial entrepreneur and regular speaker on business innovation, with an expertise in the green industry. He created his first company at age 17 and later founded Holganix, a manufacturer of 100% organic plant probiotics. He has lectured at the London School of Business, the India School of Business and the Massachusetts School of Business. He's also the co-author of the Harvard Business Review *article* Break Your Industry's Bottlenecks.

Here's How Technology Is Strengthening The Workplace

In the past, many of us were convinced that the in-person workplace was the ideal model to foster company culture and maximize collaboration. While this has plenty of truth to it, even as we look at the world as "post-pandemic," we've learned that we can achieve strong culture and collaboration even through digital workplaces.

Learning this wasn't easy – it required a lot of trial and error. However, remote work environments have opened new doors and allowed businesses to try technologies they might have previously missed or ignored. These technologies include project management software, communication tools and even advanced calendars that allow employees – remote and in-person – to really plan their days.

It's also made businesses rethink cyber security. As more owners went remote, they had to figure out how to keep their business and employees secure. In the past, they may have fallen short in the cyber security arena, but now, that's not the case. As a result of adopting new technologies and ideas, they've ended up strengthening their businesses for a different kind of future.
Inc., April 13, 2021

A Different Approach To Strengthening Your Revenue

Steven Knight, an entrepreneur and *Forbes* contributor, shares his approach to strengthen revenue and the health of a business. As the creator of solutions and opportunities at Mosaic Home Services Ltd., he offers a keen insight into the topic.

While it is a big topic, he focuses on the "customer." Every business owner needs to ask, "Who do you want your customer to be?" It seems like a simple question, but it's about trying to really understand who your ideal customer should or needs to be. Avoid making assumptions about your customers and who you think you should be targeting.

It boils down to looking at your expertise. It's tempting to offer services that are loosely related to what you already do in order to target new customers, but you have to ask yourself if it's worth the time and money. Instead, double-down on customers you already serve and serve them well, then look for more. It's not easy, but in strengthening your revenue, you need to determine who and what really matters.
Forbes, May 17, 2021

4 Cyber Challenges To Keep On Your Radar

Infrastructure Attacks. These are on the rise and have the power to disrupt supply chains, as we learned with gas shortages through large parts of the United States in May. Verizon reports that a majority (about 71%) of attacks are about extorting money. The pipeline attack was a ransomware attack.

Greater Persistence. With more people working remotely, more businesses relying on artificial intelligence and automation and more devices connected than ever before, cybercriminals are looking for new ways to exploit all of these areas.

Cybercriminals Working Together. As odd as it sounds, many cybercriminals are working together more than in the past. They rely on black markets and hidden forums where they can buy the latest disruptive tools and discuss tactics.

The Internet Of Things. There are countless devices that are a part of the Internet Of Things, including thermostats, refrigerators and even defibrillators. These devices can be hard to protect from outside intrusion, and users need to be aware of the security present on their devices and avoid those that lack it.
Forbes, May 9, 2021

"This is the third cheese delivery this month. Not only do we have mice, they appear to be tech savvy."

U.S. Presidents

Biden Trump Obama Clinton Bush Reagan Carter Ford Nixon Johnson Kennedy Eisenhower Truman Roosevelt Hoover Coolidge Harding Wilson Taft McKinley Cleveland Arthur Garfield Hayes Grant Lincoln Buchanan Pierce Fillmore Taylor Polk Tyler Harrison Van Buren Jackson Monroe Madison Jefferson Adams Washington

WHY MONITORING FOR EXPOSED CREDENTIALS IS IMPORTANT

Computer Troubleshooters
TECHNOLOGY SOLVED

HOW ARE CREDENTIALS COMPROMISED?

PHISHING

- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials

WATERING HOLES

- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials

MALVERTISING

- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials

WEB ATTACKS

- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials

Passwords are a twentieth-century solution to a modern-day problem. Unfortunately, user names and passwords are still the most common method for logging onto services including corporate networks, social media sites, e-commerce sites and others.

39%
Percentage of adults in the U.S. using the same or very similar passwords for multiple online services

28,500
Average number of breached data records, including credentials, per U.S.-based company

User names and passwords represent the keys to the kingdom for malicious attackers. Criminals who know how to penetrate a company's defenses can easily steal hundreds or even thousands of credentials at a time.

A criminal dealing in stolen credentials can make tens of thousands of dollars from buyers interested in purchasing credentials. And by selling those credentials to multiple buyers, organizations that experience a breach of credentials can easily be under digital assault from dozens or even hundreds of attackers.

$1 - $8
Typical price range for individual compromised credentials

WHAT CAN AN ATTACKER DO WITH COMPROMISED CREDENTIALS?

- Send Spam from Compromised Email Accounts
- Deface Web Properties and Host Malicious Content
- Install Malware on Compromised Systems
- Compromise Other Accounts Using the Same Credentials
- Exfiltrate Sensitive Data (Data Breach)
- Identity Theft

PROTECTING AGAINST CREDENTIAL COMPROMISE

While there is always a risk that attackers will compromise a company's systems through advanced attacks, most data breaches exploit common vectors such as known vulnerabilities, unpatched systems and unaware employees. Only by implementing a suite of tools including monitoring, data leak prevention, multifactor authentication, employee security awareness training and others - can organizations protect their business from the perils of the dark web.