

TECH BYTES

AUGUST 2021

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

The dog days of summer are here: 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 items are designed to withstand high heat, but they can only take so much. If your systems are disrupted or damaged, you can also lose critical data.

Heat can damage hard 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:

- Does your business have adequate and efficient air conditioning?
- Does your technology (such as a computer or server room) have adequate air conditioning?
- Do individual devices have adequate cooling (have employees complained about weird app slowdowns)?

You never have to compromise your data or your business. There are countless solutions to help you protect your most valuable assets – and to help with your technology cooling needs.

August is when WORLD WIDE WEB month is recognized (Aug 1 to be exact). With the click of a button, chats, video calls, photos and more can be shared all over the world.

The WWW, interconnected public webpages accessed through the internet, changed the world in ways no one could have predicted. It was, at the time, difficult to even define what "it" was.

WWW

Information can be searched in seconds, news from war zones and the birth of a child can be quickly shared across all time zones with the assistance of the WORLD WIDE WEB. Once a luxury, now the web is a necessity for most homes, news organizations, businesses, cell phones and educational facilities.

Developed in 1989, and steadily gaining rapid use and acceptance by the mid-90s, the WWW opened a horizon of communication and drastic shift in life for the modern day. Where were YOU when you first logged on?



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 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.

See the full Petra Coach webinar for Break The Bottleneck at PetraCoach.com



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*





Closing the Cybersecurity Skills Gap by Working from Home?

The cybersecurity industry faces a bleak skills shortage according to a recent Workforce Study conducted by (ISC)2. Their report shows a worldwide shortage of over 4.07 million cybersecurity professionals around the world, with over a half million in the US alone. The cyber workforce needs to grow globally by 145% and in the USA by 62% if the cybersecurity industry hopes to keep up with demand. The new normal of a remote office is here to stay and this can be good news for your security operations. Staffing your company in time zones across the county, bypassing the typical "workday" schedule, all while maintaining continuity of service to your clients -- are you beginning to see the benefits?

Talent shortage is often in large metropolitan communities where there is high demand. With flexible location and remote access, and no restrictions on geography, hiring problems which were a "hard no" become obsolete and open up doors to talent and skills in every time zone that your organization may need.

-from Cornell
Forbes Tech Council



Cyber Workforce
needs to grow:
145%

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

**AVOID MAKING ASSUMPTIONS
ABOUT YOUR CUSTOMERS
& WHO YOU THINK YOU
SHOULD BE TARGETING**



CYBER Challenges

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



600 Airport Road Winchester VA 22602
4451 Brookfield Corp. Dr, Ste. 100, Chantilly VA 20151

703 261-7200
www.bluebaytechnology.com



"This is the 3rd cheese delivery this month. Not only do we have mice, they appear to be tech savvy."



This monthly publication provided courtesy of Will Sperow,
CEO of Blue Bay Technology.

OUR MISSION: To provide our clients with the same expert-level of support that we would expect ourselves; provide it in an understanding and compassionate environment; and, work to exceed your expectations.

FREE SECURITY EXECUTIVE REPORT: 8 URGENT SECURITY PROTECTIONS Every Business Should Have In Place Now!

This report will outline in plain, non-geek speak, common mistakes that most small business owners make with their computer network that cost them thousands in lost sales, productivity & computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration of these oversights.



DOWNLOAD your copy TODAY!
www.bluebaytechnology.com/security