INDEVTECH®

TECHMinutes

Your Small Business Technology Information Source!

This Issue:

Tips for Navigating Video Meetings

Video calls have become the norm, whether you're working remotely, catching up with friends, or trying to explain to your grandma how to unmute herself. To be honest, some video meetings feel like an endurance test. Bad lighting, poor audio, and distracting backgrounds can...

Read the Rest Online!
https://bit.ly/4jBIgY1

About Indevtech Incorporated

We are the IT department for many small businesses in Hawaii, across different verticals such as healthcare, legal, financial, and manufacturing concerns.

Visit us **online** at:
newsletter.indevtech.com

The 80/20 Rule Of AI in IT Service Delivery

Why the Future Belongs to Elite Engineers.

Artificial intelligence is rapidly transforming IT service delivery. Tasks that once took hours are now resolved in seconds through automation and self-service tools. We're entering an era where the routine is handled by machines, and only the most complex, high-stakes problems reach a human.

The New 80/20 Rule

This is the new 80/20 rule: **80% of IT issues will soon be resolved by AI**, while the remaining **20% will demand the attention of a human engineer.**

AI in IT Support: What's Changing:

- 80% of common IT issues are becoming automated
- AI handles routine tasks like resets, access, and installs
- Self-service and chatbots reduce ticket volume
- Speed and efficiency are improving dramatically
- Human engineers are being reserved for the most complex issues

But this shift isn't just about quantity—it's about urgency and complexity. The issues AI can't solve don't follow a script. They involve nuance, emotion, or unique

(Continued on page 3)

Employee Spotlight: Kemis Hancock

I'm a proud Texas native, recently stationed here in beautiful Hawaii. It's been an incredible blessing to experience island life and embrace the local culture. My journey at Indevtech has only just begun, but I'm already energized by the opportunities ahead.

My background is diverse, ranging from serving in the U.S. Army to stepping in as a substitute teacher in local schools. But my most cherished role was being a stay-at-home mom for over 13 years. I returned to the workforce four years ago with a renewed sense of purpose, bringing with me a unique blend of adaptability, strategic thinking, and heartfelt communication. Every position I've held has shaped how I lead, support, and contribute—both professionally and personally.

At Indevtech, my goal is to keep executive operations running smoothly, strengthen internal communications, and help bring major initiatives to life—like our exciting 25th anniversary celebration. (See you on the green for that one!) I thrive in environments where collaboration, growth, and purpose, fuel a team—and that's exactly what I've found here. Indevtech is a company that values people just as much as performance.

(Continued on page 2)

Ransomware Is the Worst Type of Malware

Ransomware has evolved from a rare cybersecurity issue into one of the most damaging threats facing small businesses today. It's no longer just a problem for large corporations with deep pockets. In fact, small businesses are increasingly being targeted because they often lack the sophisticated defenses of larger organizations. Ransomware doesn't discriminate, and for a small business, a single attack can be catastrophic.

Let's explore why ransomware is such a serious threat to small businesses and what makes it so dangerous.

It Can Shut You Down

Ransomware works by locking you out of your systems or encrypting your data so you can't access it. For a small business, where day-to-day operations often rely heavily on access to customer records, financial documents, scheduling tools, and communication platforms, this can bring productivity to a halt. Unlike big companies that might have backup systems or alternate operations, most small businesses are not set up to function without their primary systems. A sudden shutdown means lost revenue, lost customer trust, and mounting pressure.

Costs Can Be High

The ransom itself can range from a few thousand to hundreds of thousands of dollars. But even if a business decides not to pay the ransom—which is often advised—the costs don't stop there. There's the cost of downtime, loss of data, possible legal fees, public relations efforts, and the expense of recovering and securing systems. For small businesses that typically run on tight budgets, these costs can be overwhelming and sometimes unrecoverable.
Paying the Ransom Isn't a Guarantee
One of the biggest misconceptions about ransomware is that paying the ransom guarantees you'll get your data back. Unfortunately, that's not always true. Many businesses pay up only to find the decryption key doesn't work, the criminals disappear, or the data is partially restored but corrupted. Worse still, paying once can make your business a target for future attacks, as hackers may assume you'll pay again.

Trust Is Hard to Rebuild

When ransomware hits, your customers may be directly impacted. This is especially true if their personal information is involved. This creates a double threat: not only does it open the door to possible lawsuits and regulatory action, but it also erodes the trust you've built with your customer base. A small business often relies on its reputation. A data breach can seriously damage both.

Lack of In-House IT Resources

Unlike large enterprises, small businesses often don't have dedicated IT teams to proactively monitor threats and secure networks. This makes it easier for cybercriminals to find vulnerabilities, such as outdated software, weak passwords, or employees who might fall for phishing scams. Without a solid defense strategy and immediate response plan, small businesses are more likely to suffer long-term consequences from an attack.

What Can Small Businesses Do?

Ransomware is a real and present danger, but it's not unbeatable. Small businesses can significantly reduce their risk by taking a few important steps:

- Regularly back up data and store it offline or in a secure cloud.
- Train employees to recognize phishing scams and other common attack methods.
- Use up-to-date antivirus...

Read the Rest Online!
https://bit.ly/3YB27yi

Employee Spotlight: Kemis Hancock

(Continued from page 1)

A fun fact that often surprises people: I've had the honor of being a surrogate for two families, helping bring four beautiful lives into the world. It's one of the most meaningful experiences of my life. Outside of work, you'll find me crafting with my daughter, relaxing on the beach while listening to the waves, or geeking out over the latest gadgets (I love a good gadget). I find joy in the little things and take pride in helping others find the silver lining—even when all they see is gray.

In many ways, my professional life is just getting started. For so long, I focused on making sure everyone else was cared for and where they needed to be. Now that it's my turn to shine, I'm grateful that this new chapter begins here at Indevtech.

Share this Article!
https://bit.ly/4dAgqJR

The 80/20 Rule Of AI in IT Service Delivery

(Continued from page 1)
technical challenges that require judgment and adaptability. It might be a critical system failure with no clear cause, a user locked out due to layered permission issues, or a security event that demands immediate human response.

AI is fast and efficient, but it can't reassure a panicked user or navigate ambiguity in real time. That's why the final 20% of problems won't just need human input—they'll require **top-tier support.**

Why Top-Tier Humans Still Matter

- The remaining 20% of issues are urgent and nuanced
- AI can't handle ambiguity, emotion, or unique scenarios
- Users facing critical problems won't wait for slow or poor support
- Frontline engineers must be highly skilled and communicative

And when a user reaches a human, it's not for something minor. They've already tried AI. They've already hit a wall. Now they need real help—fast. They won't wait in a queue, tolerate a script, or settle for someone who's "still learning." They expect someone who listens, understands, and fixes the issue with confidence and speed.

In this AI-driven world, **there is no room for average support.** The humans who remain on the front lines must be elite—technically sharp, emotionally intelligent, and calm under pressure. AI will handle the routine. What's left are the problems that matter most—and they demand the best.

AI is changing the game by eliminating the routine. What's left are the issues that matter most—and the people handling them must be ready.

What This Means for You

If you're responsible for IT decisions in your organization, now is the time to evaluate your support model. Is your provider keeping up with automation and AI? Are they evolving their workflows and improving efficiency where it makes sense? Most importantly, are they investing in people—high-performing, highly capable engineers—who can step in when AI can't?

The future of IT support is hybrid: automated where possible, human where necessary. The winners will be the providers who can deliver both—with excellence.

Make sure yours is one of them.

Share this Article!
https://bit.ly/4ktuNSx

Don't Get Perpetually Stuck with Break/Fix IT

Imagine owning an elevator and only fixing it when it completely breaks down. Sounds ridiculous, right? Well, that's basically what businesses do when they rely on a break/fix IT strategy.

Break/fix IT is exactly what it sounds like, you don't call in the experts until something goes wrong. On the surface, it might seem like a way to save money, but in reality, it's a recipe for stress, lost revenue, and major headaches. Let's talk about why this approach just doesn't make sense anymore.

Downtime is a Business Killer

Think about all the ways your business depends on technology; emails, transactions, inventory, customer communication. Now, imagine all of that suddenly stopping because your network crashes. Every minute your systems are down, you're losing productivity, sales, and probably some patience, too. Trying to fix things after the fact isn't just a hassle, it's expensive.

Small IT Issues Become Big, Expensive Nightmares

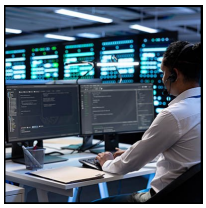
In IT, tiny problems rarely stay tiny. A small security flaw can quickly turn into a full-blown data breach. A slow computer today could turn into a dead computer tomorrow. When you're not keeping up with regular maintenance, you're basically rolling the dice and hoping nothing explodes. Something always does, however.

Break/Fix is a Money Pit

At first, break/fix IT seems like a budget-friendly option, you only pay for IT help when something goes wrong. But when things do go wrong, you're hit with unpredictable, sky-high costs. Emergency fixes aren't cheap, and you're stuck waiting for someone to be available. Instead of a predictable IT budget, you get random, unexpected expenses that mess with your bottom line...

Read the Rest Online!
https://bit.ly/4czgOYB

RMM is a Big Part of Today's Proactive Technology Management



Technology plays a critical role in how businesses operate today. From websites and servers to email systems and cloud applications, most companies rely on a wide range of digital tools to stay productive and competitive. But what happens when something suddenly stops working?

That's where IT monitoring comes in; and it's more important than many people realize.

What Is IT Monitoring?

IT monitoring is the practice of continuously checking and analyzing the performance and health of a company's technology systems. This includes things like servers, networks, software, and even individual devices.

The purpose of IT monitoring is to detect issues early. For example, if a server is starting to run out of memory, or a website is loading slower than usual, monitoring tools can catch these problems before they get worse. These tools collect data in real-time and send alerts when something isn't working the way it should.

Fixing Problems Before They Grow

Proactive maintenance is all about being one step ahead. Instead of waiting for a system to crash or for customers to complain, businesses use the information from IT monitoring to prevent problems from happening in the first place.

Why It Matters for Businesses

Downtime is costly. It can lead to lost sales, frustrated customers, and wasted time for employees. That's why proactive maintenance supported by IT monitoring is so valuable.

Here are a few key benefits of a comprehensive it monitoring strategy:

- **Early detection** - Problems can be identified and addressed quickly, often before users are even aware of them.
- **Faster response time** - With real-time alerts, IT teams can act immediately, reducing the time it takes to resolve issues.
- **Improved planning** - Businesses can schedule repairs or updates during off-hours instead of reacting to sudden failures.
- **Better security** - Monitoring systems can help detect suspicious behavior that might signal a cybersecurity threat.
- **Uptime** - Systems stay online longer, which keeps the business running smoothly and customers satisfied.

Not Just for Large Companies

Many small and medium-sized businesses think IT monitoring is only for large corporations, but that's no longer the case. Today...

Share this Article!
https://bit.ly/4cKrcwH

Indevtech has been serving Hawaii since 2001, providing end-to-end managed IT services to small- and medium-businesses. Our philosophy is very simple: we strive to be the best at what we do, so that you can succeed at what you do. We have a proven framework that, when deployed with a solid commitment from our clients, provides an unshakable foundation on which our clients can build their businesses.

Free Whitepaper:
10 Benefits of Managed IT Services
indevtech.com/10-benefits

Tech Trivia
90% of companies are unaware of their print-related costs.

Indevtech Incorporated

Pacific Guardian Center, Mauka Tower
737 Bishop Street, Suite 2070
Honolulu, Hawaii 96813-3205

Phone: (808) 529-4605

facebook.indevtech.com
X.indevtech.com
newsletter@indevtech.com
blog.indevtech.com

Visit us **online** at:
newsletter.indevtech.com