INSIDER SCOOP

On October 22nd, our team member Ally welcomed the newest member of our ohana, Colton, into the world. We're excited for her and her family!

Project Hawaii's mission is to enhance the lives of homeless children throughout the year by providing interactive programs. Our goal is to help them escape their cycle of poverty by helping them gain self-esteem, build life and social skills and keep them healthy.

For more information & volunteer opportunities, visit https://www.helpthehomelesskeiki.org/

TECH TALK

6 THINGS SUCCESSFUL PEOPLE DO RIGHT BEFORE GOING TO BED

READ – Many of the world's most successful people are big readers. They take time every night to read, which sharpens creative and critical thinking skills.

AVOID TECHNOLOGY – They shut off electronic devices and let the brain relax. Blue light from our devices, including TVs and smartphones, makes it hard for our brain to prepare for sleep and can be very disruptive.

WALK – A few minutes of walking just before bed helps to reduce stress and anxiety. Walking is another great way to decompress after a long day.

MAKE LISTS – We all have things we need to do tomorrow. Writing these tasks down gives our brains one less thing to think about, which equals better sleep.

MEDITATE – Ten minutes of meditation can do the mind and body good. Apps like Calm can help you focus and achieve inner peace before bed.

REFLECT – Specifically, reflect on what went well. Going to bed with positive thoughts is a great way to elevate your mood and stay motivated. Keep a gratitude journal and write down what went well that day before going to bed.

DON'T MAKE THIS $10,000-AN-HOUR MISTAKE

If your network fails or you experience a power outage, your business will come to a screeching halt. You're not making sales or communicating with clients. You're basically inaccessible until everything comes back online.

Over 50% of businesses take more than one hour to get back up after a crash or power outage. And who knows how long the outage may last. Each hour down is an estimated loss of $10,000. While power outages are a major contributor to downtime and lost money, other causes include failing or aging technology and buggy applications.

You don't want to put yourself in a position where downtime becomes an expensive risk. What can you do? Get a monitoring service! Monitoring services can keep tabs on your infrastructure and report their status 24/7. You'll know what's working and what's not, and you'll be able to respond to issues faster. That equals less downtime and less money lost.

UPCOMING EVENTS

BSides Hawaii
3/4/2020
Prince Waikiki
--

For more info on events, visit hitechhui.com/events.

HI TECH HUI NEWSLETTER

January 2020

this issue

"If your ship doesn't come in, swim out to meet it!"
– Jonathan Winters

OUR MESSAGE

LESSONS LEARNED IN 2019

Happy New Year! We're so excited to start the new year with all the crazy lessons we learned last year. Last year was definitely a year of growth, some painful, some surprising, but we wanted to spare you from the pain and share with you some of the greatest things that we learned and took away from last year.

First, here's a recap of what we did in 2019.   Last year we launched our SOC, we launched our mainland efforts and grew our team to 19 including contractors and part-time employees. Our growth has allowed us to sponsor children from 3rd world countries and also help some non-profit local companies. One of our favorite foundations is Project Hawaii, (please read more in our Insider Scoop section).

This year we've done more outlook migrations than we can count and we've dealt with windows end of life. We've also had way more threats to Hawaii businesses than we've ever seen!

LOREN'S LESSONS

1. Don't assume newly purchased hardware will work just because it's new!
2. Don't wait until software goes "end-of-support" to upgrade. It will be more expensive and stressful the longer you wait
3. For IT managers with tech backgrounds...learn to speak CEO. Understanding tech is not enough. You need to understand business cases, budgets and timelines.
4. Virtualize when possible. Bare metal operating system installations should be a last resort.
5. The cloud is more secure, reliable and redundant than 80% of all business networks. Not moving to the cloud because of security and availability concerns is typically a misconceived notion.
6. Most cloud security breaches are due to misconfiguration by the customer. Be sure to have a professional (like HTH! ;)), review your cloud deployment.

ANNE-MARIE'S LESSONS

1. Have weekly, monthly and quarterly processes. Have a process for everything. This includes updating and checking your AV on all machines, patching on a regular schedule, and planning company meetings.
2. Create a system of checks & balances for those processes to make sure they are being implemented.
3. Plan ahead of growth. Anticipate your resource needs AHEAD of time. When you really need the help, it will be too late.
4. Don't just be prepared, be over prepared to avoid the overwhelm.
5. "There's is always more you can do and achieve. "You Didn't Only Come This Far, to only come this far" - Jesse Itzler

CHUCK'S LESSONS

1. You can't micromanage your team and be successful. Delegating with clear instructions and expectations and trusting in your team members helps everyone grow.
2. Partnerships can be key to growth. HI Tech Hui can attribute much of our growth to our fantastic partners.
3. Don't upset your customers. Reflecting on our core values, we never want to stop "WOWing" our customers because we're busy, or make them feel like we've outgrown them.
4. Cybersecurity is not a product or a solution, it's a strategy. What's the point of having all the right security tools when you can not correlate or take action on the data that is being presented. You can have the best firewall and antivirus out there but if it's not configured correctly and re-validated on a regular scheduled basis then it can all be obsolete.
5. Most companies are NOT taking cybersecurity seriously. This could be your local stores that you shop at (and give your credit card to), your vendors, or your contractors. Be careful, don't be afraid to train and educate.

SHINY NEW GADGET OF THE MONTH

Dyson Pure Hot + Cool Air Purifier

The Dyson Pure Hot + Cool Air Purifier takes air purification to the next level. It's a fan, space heater and air purifier all in one. It includes a HEPA filter that helps reduce allergens and pollutants as it quietly cycles air through your home or the room of your choice.

One of the best features of the air purifier is the ability to monitor your home's air quality in real time, and the information appears on an easy-to-read display. Through this display, you can actually see your home's air quality improve! On top of this, the air purifier is an Internet of Things device. Connect it to your WiFi and control it directly from your smartphone, or enable voice control through Amazon Alexa.

4 Things You Should Absolutely Demand From Your IT Services Firm

How much do you rely on your IT services provider? It's startling to think that a lot of Hawaii businesses outsource their IT (which is a good thing), only to get little to nothing out of that relationship. Why? One of the reasons is that, some businesses aren't proactive. They only rely on their IT services company when there's a problem. If the network is down or their website gets hacked, they'll call their IT people, but that's the extent of the relationship.

And on the other side, there are a lot of IT companies and consultants that just wait around for that phone call. They don't work with their clients as closely as they should. Both of these reasons are downright irresponsible. First and foremost, business owners should work closely with their IT pros. They should have the staff and resources to not only address your IT emergencies but also to keep your business safe and secure to minimize those emergencies. Here are four things you should ask of your IT services provider.

"Keep my business safe!" Your IT company should make sure your network security, firewalls, malware protection, etc., are installed, operating and up-to-date. They should be working with you to do everything to keep your business's data secure and make sure it can be restored WHEN data loss does occur. Keeping your customer data secure should be a top priority. Don't take unnecessary risks, because when you do, the consequences can be devastating.

"Help me keep costs down!" You outsourced your IT to save money. Hiring an internal IT person or staff is a massive expense (plus, how many local businesses have the revenue to sustain full-time IT personnel?). However, your IT company should be working to maintain your network and associated hardware and software. They are there to help you avoid costly disasters like data loss or network downtime. If you do a lot of business on the internet, your IT company can be an invaluable asset. You literally pay them to save money.

"Help me stay proactive!" An experienced IT company has the experience and tools to spot an issue before it becomes an issue. They keep your network updated and maintained, and they can help you avoid unnecessary downtime. Working closely with your IT company means you aren't skimping on security, and this alone puts you ahead of so many other businesses that do. And make sure you have an open line of communication between your business and your IT team, even if that means scheduling regular calls. You should regularly talk about security and know about the issues that may impact your business, whether it's an equipment concern or a hacker threat. On top of that, tell your customers you care about the security of your business and their data. They will appreciate it – seriously!

"Keep my network up-to-date!" This covers a lot of ground. Your outsourced IT should be keeping your security updated, from your firewall to your malware protection, but they should also be keeping your network devices updated too. Hackers look for weaknesses in network devices every day – weak spots that allow them to capture data from your network. Sometimes they exploit the firmware, and sometimes it's the hardware. Regardless, you should always rest assured that your IT company is doing everything they can within the budget you set to keep your network as updated as possible.

If your IT company isn't doing any of these things, you need to get on the phone with them NOW! Don't put your business at risk because you only make the call after the worst-case scenario has occurred. Waiting until something breaks is a dangerous – and costly – way to do business. It's time to be proactive and get the most out of the relationship you have with your IT company.

The Shocking Truth Behind The Growing Cybercrime Threats You Face...

And What You Can Do NOW To Protect Your Company

Are businesses losing the war on cybercrime? One recent article on ZDNet says yes. The number of security breaches has risen by 11% just in the last year. This is costing businesses even more in lost revenue dealing with these kinds of attacks. It's wasting their time and resources.

In 2016, Cybersecurity Ventures stated that by 2021, digital crime will cost businesses a total of $6 trillion. So far, this projection seems on point as hackers continue to chip away at businesses around the world. They don't care about the damage they're doing.

Right now, the Internet is flooded with sensitive data. From passwords to financial information – it's out there. Some of it is secure, some of it isn't. Either way, because of the sheer amount of data floating out there, cybercriminals have a greater chance to get what they want. And over time, it becomes harder to protect that data.

But the cyber security industry has also grown in response. People are fighting back. In 2018, the investment into cyber security totaled $37 billion. However, it seems like it's just not enough. When you look at small and medium-sized businesses – the targets of nearly 70% of cyber-attacks, according to SMB Group – cyber security isn't taken as seriously as it should be.

In 2017, Harvard Business Review looked at the reasons behind why many businesses don't take cyber security seriously. The results were interesting. It turned out, businesses don't treat cyber security as "the ongoing process that it is." Instead, it's typically treated as a "finite problem that can be solved." In other words, if you do the bare minimum for security today, the thinking goes, you'll be protected tomorrow.

The problem is as the Internet changes and evolves, so do the threats against its users. It's pretty much impossible to set up a one-and-done security solution. If you were to set up something like an SMB "quick fix" and walk away, there's a good chance your business would be the successful target of an attack within a matter of months.

This kind of thinking is far more costly than many business owners realize. A study by Akouto and Alpha Logistics found that businesses that underinvest in cyber security end up spending more on cyber security in the long run as they deal with attacks – up to 58% more. These costs don't even include downtime or lost wages caused by data breaches. In short, recovering from an attack is FAR more expensive than investing in security now.

So what can you do to protect your business? You can start with changing the way you think about cyber security. You have to accept that the threats are out there and will always be out there. But there are things you can do to minimize those threats.

Start with your people. For many businesses, especially those smaller than Fortune 500 companies, your biggest threat is right inside your organization. For those of us who are Internet-savvy, most would never dream of clicking on a scammy link or responding to a phishing e-mail. We've been around the cyber block and we know what to look for.

However, people still fall for even the most basic scams. There will always be someone on your team who isn't informed about these kinds of threats, or those who use obvious passwords. ZDNet points out that "only 26% of workers know what to do in the event of a breach" and that "7% openly acknowledge that they ignore or go around security policy."

It pays to invest in a thorough and ongoing training program. It's crucial to outline clear and firm security protocols so your team knows EXACTLY what to do. No one's left guessing or clicking on anything they don't recognize.

It's also crucial to not go it alone. The single best way to stay on top of all things cyber security is to hire a highly experienced managed services provider who is up-to-date on the threats you're facing. Having a partner means you don't have to assume your business is protected. You'll know your business is protected.

OUR SOLUTIONS

BlackBerry
CYLANCE.
SOPHOS
ControlScan
Fidelis Cybersecurity
FIREEYE
DEMISTO
JUNIPer NETWORKS
thycotic
DARKTRACE

CONNECTIONS

Connect with us on social media

Call us at
808.206.8549
or email us at
info@hitechhui.com