HI TECH HUI NEWSLETTER

June 2020

this issue

Our Message P. 1

3 Ways To Stop Cybercriminals Cold In Today's Crazy Times P. 2

Who Is Responsible For Your Corporate Culture? P. 3

Insider Scoop P. 4

Tech Talk P. 4

"Strength does not come from winning. Your struggles develop your strengths. When you go through hardships and decide not to surrender, that is strength."
—Arnold Schwarzenegger

OUR MESSAGE

As some of you know, HI Tech Hui is now fully operational with our very own 24x7 Security Operation Center (SOC) which we've branded under CYBERUPTIVE. We are using the 'follow the sun' methodology, with our East Coast operations taking over while our Hawaii operations are sleeping. With our multiple shifts and 2 locations, we're able to cover 24 hours a day, 7 days a week.

Always think, "it's not a matter of IF I get breached, it's a matter of WHEN I get breached..."

In the wake of **COVID-19**, we're seeing an increase in cyber attacks, mostly in Russia and China. There has been an apparent increase in; reconnaissance, intelligence gathering from outside the country, collecting intel on your network, and checking for open ports or exploits and opportunities to attack. Before, you could use geoIP blocking to block those countries, now machines are spinning up in different data centers in the US performing the same intelligence gathering. They are using US based servers, trying to launch attacks on different US companies.

We're seeing a huge increase in spearphishing and very specific targeted attacks. Usually, they are really easy to figure out, but the latest rounds are getting harder to decipher. The attacks are also happening "off hours". Friday nights and weekends are producing an increase of attacks.

Colleagues in the industry are saying that ransomware is coming back with a vengeance. Always think, "it's not a matter of IF I get breached, it's a matter of WHEN I get breached..."

Make sure you have a process to check daily backups. Turn on MFA for everything. In the beginning of the month we saw a bunch of password spray attacks for O365 accounts that didn't have MFA enabled.

In the last year we as well as our partners have discovered:

- 41% of malware that was seen is brand new and has never been seen before
- 70% of all samples came from 5 malware families
- 23% of the malware is publicly available, and can be used by various skill sets

The most common malware we have seen are:

- Trickbot - A modular banking trojan that uses web injects. - Credential Stealer
- Qakbot - Banking Trojan been around since 2008
- Beacon - An open-source endpoint agent for Cobalt Strike, is used by APT19, APT32, APT40, APT41, FIN6, and FIN7
- Empire - An open-source post-exploitation framework and PowerShell endpoint agent. Provides Keyloggers and software such as mimikatz.

So for us at HI Tech Hui, we've not only been battling the COVID biological virus, but we're also battling a significant increase in cyber viruses. Many businesses in Hawaii right now are going through some hard times, the last thing we need are more cyberattacks to knock us down even more. Our desire to protect and help Hawaii's businesses is why we worked so hard to build our very own SOC.

- Chuck Lerch

Who Is Responsible For Your Corporate Culture?

"Corporate culture" is the fundamental character or spirit of an organization that influences the loyalty and general behavior of its employees. When you learn how to combine the right corporate culture with the right core values, your organization will thrive regardless of the challenges it faces.

One problem I see in most companies today is they create a mission statement only because it's fashionable to do so ... but they stop there. Some may even go so far as to create a list of core values to help guide their leadership and employees ... but they fail to follow them. I see lots of mission, vision and value statements on corporate websites, but the majority of employees in any company cannot recite any of them.

Several months ago, one of my clients wanted me to work with their senior management team to identify ways they could create better employee engagement. An anonymous survey was conducted, and it turned up some alarming comments. Over 50% of their employees stated that the company:

- Isn't results-oriented
- Doesn't celebrate accomplishments
- Doesn't have training for growth
- Doesn't allow them to generate ideas
- Isn't empowering them
- Has leaders who play favorites
- Has leaders whose actions do not match their words
- Doesn't involve them in the decisions that affect their jobs
- Doesn't keep them informed about changes or important issues

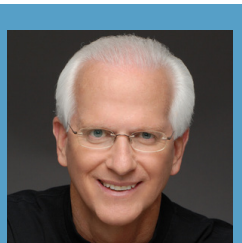
This company has five excellent "Guiding Principles" (core values) that address all these issues, but they weren't being followed. What most companies don't understand is that their "corporate culture" is in the hands of local middle management. In other words, your corporate culture is your LOCAL BOSS. They are responsible for making sure your guiding principles, core values, and mission and vision statements are being followed.

Last week I did a program for Herr Foods. Herr Foods understands the importance of living their core values. They have been in business for over 70 years and have over 1,500 employees. Their formula for success is based on the acronym

L.O.V.E., which stands for:
L - Live
O - Our
V - Values
E - Every day

A recent Gallup poll found that only 34% of workers are committed to their company and are enthusiastic about their work. That means 66% are NOT engaged; they are just going through the motions, collecting a paycheck. As you look to the future, recognize that the principles that are instrumental to your success must be communicated throughout your organization on a constant basis. They should not only be part of your new employee training; they should also be part of every meeting, deeply rooted into every decision you make.

When your corporate culture is right, employees working for you no longer have jobs; in their minds, **THEY HAVE CAREERS.**



Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys and 52 Essential Habits For Success, he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Tony Robbins, Tom Peters and Stephen Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.

OUR SOLUTIONS

BlackBerry
CYLANCE
SOPHOS
Fidelis Cybersecurity
FIREEYE
JUNIPER NETWORKS
DEMISTO
thycotic
DARKTRACE

CONNECTIONS

Connect with us on social media

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

SHINY NEW GADGET OF THE MONTH

Zepp Golf 2 Swing Analyzer

Improve your golf game with a device smaller than a golf ball. The Zepp Golf 2 is a remarkable piece of tech that attaches to the back of any golf glove. It's packed with sensors and delivers real-time analysis of your game.

Using Bluetooth, the Zepp Golf 2 pairs with your smartphone. As the data is analyzed, it's displayed on the accompanying app. It tracks your club speed, backswing positioning, hip rotation, consistency and much more. The Zepp Golf 2 also has a long-lasting battery – up to eight hours – so it will definitely make it through your next game without a hitch. The Zepp Golf 2 is compatible with both iPhone and Android devices. Learn more at Amazon or Zepp.com.

3 Ways To Stop Cybercriminals Cold In Today's Crazy Times

You've seen it. You've probably even experienced it. For what feels like forever now, just about everyone has been forced to modify priorities. As a business owner, you've probably been focused on shifting your business to accommodate this world crisis. You may even be investing more of your time in retaining customers and generating new cash flow. If you're like most people out there, you've barely even had time to think about cyber security and protecting your important data.

Maybe you've heard the saying "Never let a crisis go to waste." It's as if cybercriminals wrote it because that's exactly what they're thinking right now. In fact, they're probably working overtime right now to craft new malware while our lives have been turned upside down. Yes, as you're focused on your business, hackers are finding new ways into your IT network. Their objective is to steal data and passwords, compromise your clients' private information and even demand large ransoms.

Did you know that cybercrime is expected to cost $6 trillion (that's a 6 followed by 12 zeroes!) by the year 2021? But, now is when hackers are expected to do their absolute most damage.

Here are three strategies you can use right now to help protect your business data, money and productivity during these unusual times.

1. Guard Your Inbox.
People aren't paying as much attention as they usually do, which makes it the perfect time for cyberattackers to send e-mails with dangerous malware, worms and viruses. Always carefully inspect every e-mail received and make sure you know the sender.

Here's another tip: avoid clicking links in the e-mail unless it's abundantly clear where they go. Also, don't ever download an attachment unless you know who sent it and what it is. While it takes a few extra seconds, double check by calling the person who sent you the attachment. Better safe than sorry. Make sure you communicate these safeguards to everyone on your team, especially if they are working from home.

2. Secure Your Company-Based Technologies.
During crises like this one, your passwords are a critical first line of defense. Don't wait for your company's finance data to be compromised. Make a point now to reevaluate your passwords and direct your team to create stronger passwords. Too many employees are guilty of using the same password across multiple applications. Use a unique password for every single application.

Your team may tend to save your passwords in their web browser. Don't do this. A skilled hacker can bypass the PIN required to access your saved passwords. Once they have the password or PIN to access your web browser, they can steal as much as they want – credit card information, customers' private data and more!

We recommend our clients use a password manager. It's convenient, but more importantly, it's far more secure.

3. Secure Your Home-Based Technologies.
With the coronavirus pandemic, far more businesses are encouraging their employees to work from home. That means a lot of people are working from the living room or kitchen without giving a second thought to security. This negligence is an invitation to new cybercrimes.

Here are a few tips to ensure your work-from home employees are keeping your network and data secure: make sure your employees and contractors are not using their home computers or devices when they are working from home. Add a firewall to ALL computers and devices that will be utilized at home. Finally, your network and data are not truly secure unless your employees utilize a VPN (virtual private network).

There's no need to invite in more problems by letting your computer and network security slide during these times. We would be happy to help you create or even improve your work from home environment.

While this coronavirus scare has negatively affected countless businesses, we are proud to say we are open and continuously servicing your customers. If you need additional security advice or would like to have a consultation to discuss how to keep your data safe or how we can help you work more effectively, simply connect with us today.

INSIDER SCOOP

Here are some of our COVID-19 internet shopping splurges. What have you bought lately??

We are addicted to ALLLLLL the subscription boxes right now!

And apparently we have an affinity for Vinyl Records!

We love ALL the things!

UPCOMING EVENTS

--

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

TECH TALK

Do These 3 Things To Make Sure You Don't Get Hacked

1. Train up. Get your entire team trained on IT security fundamentals and best practices. They should know how to create strong passwords, how to safely access the web and how to securely use e-mail – including how to identify phishing scams. They should have a clear understanding of today's threats and how to be proactive inaddressing those threats.
2. Invest in good tech. You should be invested in solid malware protection, including antivirus software and firewalls. All of your data should be backed up to the cloud and expertly secured using encryption software. You should also be invested in threat monitoring.
3. Establish relevant systems and processes. Have standard operating procedures (SOP) in place to train employees, respond to threats and access networks. For example, are employees connecting with unverified devices from home? Establish rules on what can and cannot happen. Another example: are your cloud backups set up correctly? Is someone checking it? Again, have SOP in place to address these kinds of issues. *(Small Business Trends, Feb. 13, 2020)*