THE INTEGRATED AXIS TECH CHRONICLE

What's New

FREE Executive Webinar

Five Steps to Improve Your Cybersecurity Posture

Webinar Details: LIVE Wednesday, March 8th & 22nd, 2023

Start Time: 10:30 - 11:30 a.m. Arizona Time

With Presenters:

Paz Terry

Michael Lazar

Register here

CARE²

Customer Focus
Accountability
Respect
Excellence & Empathy

March 2023

This monthly publication provided courtesy of Sean Oseran, CEO of Integrated Axis Technology Group

Improve Your Cyber Security Awareness

Learn About Today's Most Common Types Of Cyber-Attacks

If you've turned on the news sometime during the past few years, you've probably heard of more than one instance where a business closed due to a cyber-attack. You may think your business is small enough and hackers won't target you, but this couldn't be further from the truth. Every business is at risk of experiencing a cyber-attack and should be well-prepared to defend against these threats. With the right type of attack, a cybercriminal can gain valuable information about your business, customers and employees, which can be used to damage your reputation and hurt you financially. If you're a business owner or leader and you want to ensure your business is well-protected, check out the most common cyber-attacks that are affecting companies today. From there, you can implement cyber security plans and tactics to ensure your business is protected from cybercriminals.

Phishing Scams

Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure. Phishing scams can wreak havoc on your business and personal life. You may have seen an e-mail from someone claiming to be Amazon or your credit card company asking for specific sensitive information. Often, the e-mail address does not line up with who the person is claiming to be.

When a phishing scam targets your business, they'll likely request valuable information from your employees such as passwords or customer data. If your employees fall for the scam, they could give a cybercriminal unprecedented access to your network and systems. This may also allow the cybercriminal to steal private employee and customer information, leaving your employees

Continued on pg.2

vulnerable to identity theft. Phishing scams can be averted by using common sense and providing cyber security training to your employees. Most companies will not request private information over e-mail. That being said, if an employee receives a suspicious e-mail, they should do their due diligence to ensure the e-mail is genuine before responding in any way.

Malware
Malware is software installed on a computer without the user's consent that performs malicious actions, such as stealing passwords or money. There are many types of malware, including spyware, viruses, ransomware and adware. You can accidentally download malware onto your computer by clicking on sketchy links within e-mails or websites. You might not even notice you have malware on your computer right now. If your computer is operating more slowly than usual, web browsers are taking you to random sites or you have frequent pop-ups, you should scan your computer for malware.

Prevention is key in stopping malware from affecting your business. Hiring and utilizing a managed services provider is the best way to protect your business, as they will continually monitor your network for exploitable holes. With malware, it's always better to play it safe than sorry. If a cybercriminal is able to use ransomware on your network, your business could be stuck at a standstill until you pay the ransom. Even if you can pay the ransom, your reputation will still take a hit, and your business could be greatly affected. Be careful where you click on your phone, too, since malware attacks on cellphones have become more common over the past few years.

Attacks Involving Passwords
How do your employees access your network or computer systems? They most likely use a password to log in to their computer, access their e-mail and much more. What would happen if someone with bad intentions gained access to one of your employee's passwords? Depending on the individual's access, they could obtain sensitive information about your business, customers and employees.

Your team should be using long, complex passwords for their accounts, and each password for every account should be different. Encourage your employees to use password managers that will allow them to create the most complex passwords possible and keep track of them more easily. You can also incorporate multifactor authentication to ensure nobody can steal a password and gain access immediately. You should make your employees aware of this during your annual cyber security training.

If your business falls victim to a cyber-attack, it could have lasting consequences for everyone involved. Now that you know the most common types of cyber-attacks, you can start implementing plans to ensure you and your business stay protected.

> Every business is at risk of experiencing a cyber-attack and should be well-prepared to defend against these threats."

Security Awareness Training

It's vital for businesses to keep their networks free from security breaches and safeguard their data. Central to this goal is educating staff on best practices and what to look out for using security awareness training.

72% of businesses have been affected by fraudulent emails and 52% of businesses have experienced a cybersecurity breach within the past year. On average, it takes 120 days for a business to discover a data breach. One single incident can cost upwards of $100,000 in terms of lost revenue, recovery of assets, and fines. These alarming statistics convey a clear message when considering investing in preventative and proactive measures. Your business cannot afford to *not* do it.

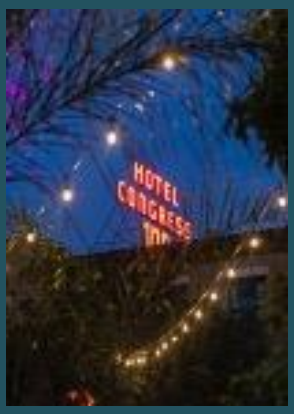
It is evident, user behavior must change. Human error is costly and the weakest security link in any organization. Quality software and staff training are not only essential, but the first and most crucial line of defense for all businesses.

There is a comprehensive solution that offers continuous dark web scanning, identifies compromised passwords, and protects against hacking attempts. IA offers security awareness training tools that run phishing simulations and educates staff on how to spot suspicious emails. It offers brief weekly training and HIPPA compliance programs to keep your team alert and vigilant. The bottom line, an educated staff keeps businesses safe.

Client Spotlight: Hotel Congress

Hotel Congress was built in its current location at 311 East Congress Street in 1918 and quickly became a central hub to the growing Tucson community. Boasting unique Southwestern charm, this cultural landmark downtown incorporates fine dining at Maynards, a rotation of talented musicians at Club Congress, and the newest addition of the Century Room where you can sip small-batch mezcals while listening to jazz.

Hotel Congress is the host of the Agave Heritage Festival, established in 2008. This year's festival includes several exciting downtown events from April 27th to April 30th.



The festival celebrates and explores the agave's cultural, sustainable, and commercial significance across borders. Events include seminars, agave pit roasting, agave spirit tastings, and world-class culinary events conducted by industry leaders, culinary leaders, and spirits professionals.

Integrated Axis is a proud sponsor of the 2023 Agave Heritage Festival, and we hope to see you there!

https://hotelcongress.com/

https://www.agaveheritagefestival.com/

AGAVE HERITAGE FESTIVAL
EST. 2008
APRIL 27 - 30

Don't Come Back To Work

Don't come back to work. Instead, move forward in leading your company and managing your career by embracing remote work. Even though ghSMART has been remote-only for over 26 years, I never fully realized how enthusiastic I am about remote work until I heard that many companies are forcing workers to come back into offices.

Before the COVID-19 pandemic, "work where you want" was a rare concept – but during the pandemic, basically every company that could function with people working remotely shifted to that mode out of necessity. I thought that mode would stick, and we'd see the landscape of cities shift from "places people go to work every day" to "places people go to work sometimes, eat, shop, learn and play." But it seems I was wrong.

There isn't a great argument against the idea of remote work, but there is one for it. Remote work improves financial and operating performance and productivity for companies while also improving job and life satisfaction for employees. A 2015 Stanford University study published in the Quarterly Journal of Economics showed a 13% performance increase from remote working, and employee attrition rates fell by 50%.

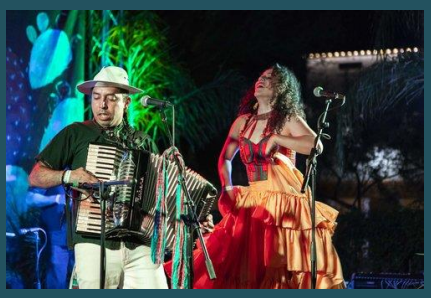
Even with all of the research and information available that shows remote work is beneficial, there are still some myths floating around. For example, many say you can't build a great company culture when your business operates remotely. This is entirely false. I think an excellent culture begins with doing what's best for people. Making people commute to offices daily does not seem to be in anybody's best interests.

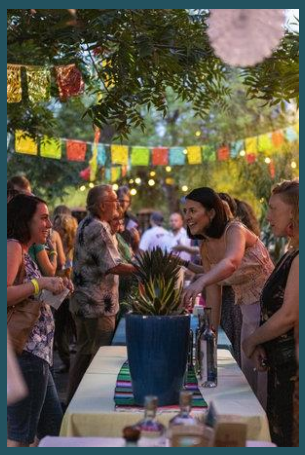
Another common myth states that people don't work as hard remotely as they do in an office. I believe that if you have a transparent culture where performance is measured, you can pay people according to the value they are creating. They will be incentivized to work productively and not lollygag – even if they are working remotely. But I guess many companies have not yet figured out how to pay employees based on a scorecard of measurable results and instead pay based on hours worked. They should be worried about lollygagging anyway, both in the office and for people who work remotely.

If you run or own a company, please continue to experiment with allowing your people to work remotely when possible. I believe this is the future of work, both because of the demonstrable benefits to companies in operating and financial performance and the benefits to workers due to having more control over their time.

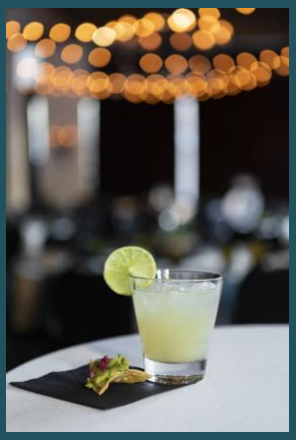
Guest article provided by:
Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times bestsellers. He stays active in his community and has advised many government officials.

Integrated Axis is a proud sponsor of the 2023 Agave Heritage Festival





AGAVE HERITAGE FESTIVAL
EST. 2008
2023



April 27th Mexican Fermented Beverages Workshop, Mezcrawl, & Agave Heritage Dinner
April 28th Spirits of Sonora Tasting
April 29th Ignite Agave Opening, Western Jalisco Tasting, & Agave Fiesta
April 30th Sotol Tasting & Lecture