THE INTEGRATED AXIS TECH CHRONICLE

What's New

Events Around Town

- Tucson Gem & Mineral Show
- Artful Connections - Desert Museum Baldwin Gallery
- Juilliard String Quartet - Berger Performing Arts Center
- Star Party - Catalina State Park
- Rodeo Festival - Tucson Rodeo Grounds

CARE^{2}

Customer Focus
Accountability
Respect
Excellence & Empathy

February 2024

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

SHOW SOME LOVE TO YOUR BUSINESS CONTINUITY PLAN

Wintertime can feel like a wonderland. There's hot cocoa, cozy fireside conversations, glistening white snowfall…ice storms, power outages and tons of employee sick days. You can't predict the future, but a business continuity plan – BCP for short – ensures that unexpected events don't slow you down because, in business, every minute counts – literally. Downtime costs SMBs $137 to $427 per minute, according to a 2020 IBM report. Although the loss is smaller, extreme downtime is the ultimate undoing for many SMBs.

This month, while you're rushing out to buy flowers or before you settle in for a cozy Netflix series, don't forget to show your BCP some love too.

What Is A Business Continuity Plan?

It's just like it sounds – a plan to keep your business continuously running in the case of an unplanned event like a natural disaster, cyber-attack or human error. A BCP outlines processes and procedures your company will follow during a crisis. It considers operations, assets, human resources, technology and safety; in other words, it keeps necessary functions in your organization running until the disaster is handled.

Isn't A Disaster Recovery Plan The Same Thing?

Disaster recovery plans focus solely on restoring your IT systems. It's one – albeit critical – component of your BCP. If a winter storm knocks out your Internet, a disaster recovery plan restores data access and any IT services you may have lost.

Continued on pg. 2

Why A BCP Is Important

Let's say your office suffers a major fire incident. Do you know where and how your employees would work? Would they be able to handle customer calls? Where would your executive team meet to make critical, time-sensitive decisions? In addition to providing a plan for restoring your IT systems, a BCP is a practical framework for your entire company's resiliency and financial sustainability.

Additionally, people want to know you have it together. If you hesitate or flounder in response to an emergency, you'll lose the trust of your team and customers, and that's incredibly hard to get back.

What Your BCP Needs

A few basic elements make up a solid BCP framework for every business, no matter your industry.

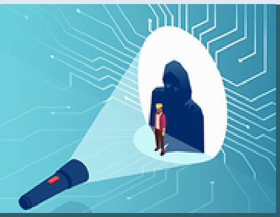
1. Your company's critical functions. What are the must-do activities in your business? This could be anything from order fulfillment to customer support. Knowing what's absolutely critical to your company helps you prioritize during a disruptive emergency. Assess the likelihood and impact of these risks to understand what you're preparing for.
2. Risk assessment. What types of crises could disrupt your business? These could range from natural disasters, like floods or earthquakes, to cyber-attacks or a key employee leaving unexpectedly. But don't linger too long on this step because you can't possibly think through every scenario – focus on recovery.
3. Recovery strategies. For each critical function and process, develop strategies to recover during a disruption. This might include alternative methods of operation, using different locations, employing backup systems, etc. Pro Tip: ditch wordy manuals and use flow charts and checklists to communicate plans to your team.
4. Data backup and recovery. Check (and double-check) that all your critical company data is regularly backed up and can be restored quickly. Decide on off-site storage and cloud backups and establish protocols for data recovery.
5. Communication plan. This includes how you'll communicate with employees, customers and stakeholders during a crisis. Who says what and through which channels? Include contact lists, communication templates and dissemination methods (e.g., e-mail, social media, website updates).
6. Alternative operations. If your main office isn't usable or accessible, where will your team work? Do you have relationships with alternate suppliers if your primary ones are unavailable?
7. Review schedule. Your business will evolve, and so should your continuity plan. Create a schedule to run drills and update your plan regularly. Also, distribute it to everyone who needs to know, so everyone knows their role during a crisis.

Is A BCP Right For Your Business?

There is absolutely no company – big or small – that's not at risk of a disaster. According to a 2022 threat report by ConnectWise, nearly two in three midsize businesses experienced a ransomware attack in the last 18 months. One in five victims spent $250,000 or more to recover. The odds are not in your favor when it comes to business risk.

Remember, the goal of a BCP is to minimize disruption to your business and help you get back to normal operations as fast as possible. Get with your team and review your BCP today. If you don't have one, consider this your sign to get it done.

CYBERSECURITY CORNER: GOOGLE HACK, IS YOUR ACCOUNT SAFE?



A recent report from a security company called CloudSEK has found a serious security issue that can let bad actors compromise Google accounts. This exploit takes advantage of a vulnerability in the way Google authorizes access, known as OAuth2. The exploit, linked to a group called PRISMA, manipulates certain codes to create long-lasting access to Google services, even if a user changes their password. CloudSEK's research team traced the problem to an undocumented part of Google's authorization system called "MultiLogin," which is meant for syncing accounts. The exploit is part of a malware called Lumma Infostealer and is cleverly designed to keep access even after a password reset. It specifically targets a part of Google Chrome's internal system to steal important information. Despite being a sophisticated attack, it continues to work even if users change their passwords, making it a big threat to the security of user accounts and data. The report underscores the concerning trend of these types of attacks spreading quickly among different hacker groups and stresses the importance of being more aware and taking extra security measures to protect against such threats. If you have concerns about cybersecurity and your business, call IA today for more information on how to stay safe!

EMPOWERING SAZ: WE CARE TUCSON

WE CARE TUCSON
refurbished electronics
& durable medical equipment

Thank you to everyone who attended our “Purge The New Year” technology recycling event in partnership with We Care Tucson! This local nonprofit is driven by the belief in a thriving, sustainable, and interconnected community.

WCT understands that access to essential resources is crucial for the well-being of individuals and the community as a whole. To turn their vision into reality, the organization focuses on providing access to information technology and medical equipment supplies.

One of the unique aspects of WCT's approach is the emphasis on sustainability. Through responsible recycling practices for non-functional components, WCT not only reduces electronic waste but also promotes a more environmentally conscious and sustainable community.

By bridging the digital divide, WCT addresses the issue of unequal access to information technology, and work to empower individuals with the tools and skills needed to thrive in an increasingly digital world. Additionally, providing access to medical equipment and supplies contributes to a more equitable healthcare landscape, ensuring that everyone in the community has the resources they need for a healthier life.

WCT's commitment to cultivating an equitable and sustainable community goes beyond providing physical resources. The organization actively engages in community-building activities, like the youth tech camps teaching school-age children about building and servicing technology equipment.

To make a donation, please go to wecaretucson.org

OLD MALEWARE, NEW TRICKS

An old malware scam is reemerging with dangerous new tricks, causing significant problems for anyone who uses a web browser – i.e., nearly all of us. Hackers using the “update your browser” scam found new ways to hide malicious files, making it harder for security experts to locate and remove them. We’ll see more of this scam, so you need to be on the lookout.

What Is The Fake Browser Update Scam?

A website gets hacked by cybercriminals, who make a few changes. Namely, hackers use JavaScript requests to covertly replace the existing website content with a deceptive prompt for a browser update. For example, if you use Chrome, you’ll see a page asking you to update your Chrome browser. Click on the update button, and you’ll download malware on your device. Hackers know that users are told in security training to only click on links on trusted sites. They take advantage of that training by hosting their scam on a legitimate site, luring you into their trick.

But this time, the scam has a new tactic. Instead of hosting harmful files on the compromised site as they’ve done in the past, they’ve developed a way to store files on cloud services or even cryptocurrency blockchain. This makes it a lot harder for cyber security experts to find and remove.

The first scam of this kind, ClearFake, was uncovered in October 2023. Since then, security experts at Proofpoint have identified four threat actor groups using the fake browser scam to attack victims.

We keep hearing it – cybercriminals are using the latest tech to find new ways to exploit users. This is just the latest example.

What Can You Do About It?

First, no browser targeted in this scam – Chrome, Firefox or Edge – will ever have a pop-up or show you a page stating your browser is out-of-date. To check your browser’s status, go directly through your browser’s settings menu. Also, make sure you’re running very effective antivirus protection on all your devices. Antivirus will constantly run on your device, alerting you to suspicious activity.

Additionally, train your team on this new scam. Because it goes against usual training, you’ll need to step in and talk to them about how to look for signs of the fake browser update scam.

We use browsers to do almost everything, so this won’t be the last time you hear about scams like this. Be sure to keep your systems updated (via your settings, NOT pop-ups) and use a strong antivirus program.