DanTech Services
Computers under control!™

Technology Times September 2024 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

Dan Foote
Owner/President

What's Inside:

The Changing Face of the Workplace: How people want to work today

Four years after Covid-19 cleared out communal workspaces, the real estate market is still feeling the economic burden of high interest rates and a decreased demand for commercial buildings.

Since the pandemic, people have altered their workplace preferences. The research from several studies gives us a prediction of the workplace of the future and offers suggestions to help businesses adapt to the new environment.

Commercial real estate:

The future of office buildings remains uncertain because employees are interacting in new and different ways; there are more vacancies in older office buildings; and environmental, social and governance factors are affecting demand.
A decade ago, real estate developers and investors were focused on properties in urban areas, targeting millennials as they graduated from universities and wanted to be near the commercial district. But that's no longer the case.

A combination of commercial and residential spaces seems to be the ideal office space today, allowing people to work and live within a community. These mixed-use environments also offer the advantage of shorter commute times and reduced carbon emissions.

Shiny Gadget of The Month

[Sweep & Swipe Laptop Cleaner](#)

If you want to spiff up your laptop, like it just came out of the box, you can use the OXO Sweep & Swipe Laptop Cleaner to wipe the screen, dust the keyboard, and remove lint from the connectors. It's also handy for other electronics, including cell phones, tablets, and desktops.

This lightweight, pocket-sized tool from OXO - the maker of inexpensive, clever household products – combines a microfiber pad and a soft brush on opposite ends of the handheld product.

The microsfiber pad is useful for removing smudges or specks from your monitor, iPhone or iPad screens, eliminating the need for a cleaning liquid.

The other side of the device contains a retractable soft brush that works well for cleaning keyboards, speaker grilles, and connectivity ports.

Its adjustable length gives you better reach into crevices. The shorter bristles are good for removing lint from the sides of cell phones.

This tool is easy to clean with just warm water, a little soap, and a paper towel to dry it.

It's also recommended that you leave it out a few hours after cleaning to let it completely air out and properly dry.

American Airlines recovers more quickly than others after CrowdStrike incident

When the CrowdStrike outage affected airlines throughout the world, one domestic airline recovered quickly and got its aircraft moving again, while others were slow to recover. American Airlines had assembled the right team to help them restore operations within an hour of the outage.

In a meeting held after the incident, American Airlines executives gratefully recognized their company's foresight in planning ahead for such an incident and in assembling a strong IT team quickly. After the outage caused from the CrowdStrike incident, many of American Airlines' operating systems were taken offline, just as happened at other airlines and businesses internationally.

Although American did have to cancel 400 flights during the first 24 hours, it only had to ground 50 flights the next day (source: flight tracker Flight Aware), making it one of the fastest domestic airlines to recover.

The global disruption led to many different reactions throughout the airline industry. The challenge for many airlines was to quickly deploy IT teams, who then had to repair systems at hundreds of airports. An individual person had to physically access each individual computer to perform the recovery process, causing some airlines to take much longer to regain operational footing, even four days after the incident.

Delta Airlines, for one, struggled to recover from the IT outage, resulting in thousands of cancelled flights and a loss of $500 million. The airline hired a legal firm to pursue claims against CrowdStrike and Microsoft for these losses. In response to Delta's lawyers, both Microsoft and CrowdStrike claimed that they reached out to the airline, offering their assistance, but received no response. And lawyers from Microsoft claim that Delta has not updated its IT infrastructure, either for the benefit of its customers or its employees. The CrowdStrike outage interrupted many of the critical services that keep airlines operating on a full-scale basis. Delta, and many other airlines depend on their numerous partner services for all aspects of their operation, including meal services, luggage transport, and crew scheduling.

So what was the key to a rapid recovery for American Airlines? Crew-tracking systems, rather than the customer-facing endpoints that other airlines relied on to get their passengers onto planes. Anytime there's a disruption, it's crucial for airlines to keep track of their aircraft and crew. And they must take action quickly, according to American Airlines executives.

Preparation and early steps lead to better outcomes in the case of a crisis. American Airlines also gave credit to having strong, reliable communication methods in place to get in touch with team members out in the field.

One executive said American was prepared for this IT crisis from their experience overcoming weather-related disruptions. The airline prioritized its operations technology investments after a winter 2022 storm grounded Southwest Airlines' entire fleet during the busy holiday season, which led to a billion-dollar loss for Southwest.

Many lessons are still being learned from the CrowdStrike outage. Details of why some airlines struggled more than others are likely to emerge from an investigation started by the Department of Transportation after the outage.

Dangerous Possibilities of a Downgrade Attack

At Black Hat 2024, cyber security researchers revealed that a fully-patched Windows computer can be "unpatched," forcing an up-to-date device to roll back to earlier software versions, and reintroducing it to past vulnerabilities. This is known as a downgrade attack.

This downgrade attack would make the term "fully patched" virtually meaningless on a Windows computer. By compromising a Windows update, this downgrade would attack critical OS components such as Dynamic Link Libraries (DLLs) and the NT Kernel, both essential for the effective operation of Windows applications and software.

A downgrade attack is undetectable by endpoint detection and response (EDR) solutions, and it fools the Windows machine into thinking that the device is fully updated. Researchers believe these findings are important not only for Microsoft, but also for other OS vendors who could be susceptible to similar attacks.

In response to these findings, Microsoft said it's working on an update to revoke outdated, unpatched system files to mitigate the attack. However, the company is not currently aware of any attempts to exploit this vulnerability.

907-885-0501

Studies indicate that office demand in median-income cities has decreased by 13%, with some cities even experiencing a decline of up to 38%. This trend is largely attributed to the growing popularity of hybrid work.

What can businesses do to adapt:

Cities and office buildings can thrive by adopting the hybrid approach themselves. Designing buildings that support hybrid workers involves creating spaces that support both in-office and remote work, fostering a productive and engaging work environment.

To achieve this, businesses can incorporate shared workspaces, designate collaboration zones, provide enclosed spaces for uninterrupted work, incorporate robust digital infrastructure, invest in ergonomic furniture and energy-efficient elements to ensure your employees are comfortable and productive.

Flexibility is crucial. Work is no longer confided to traditional office spaces. Whether at the kitchen table, the coffee shop, or the cubicle -- employees want the freedom to access whatever they need to get the job done. The workforce of today has adopted an anywhere, anytime, any platform mentality.

Flexible schedules are also essential in today's fast-past and ever-changing work environment, as they enable employees to achieve a better work-life balance and increase productivity.

Both the hardware and software elements of workplaces may need to be changed to accommodate employee preference. Higher quality workspaces have the potential to entice employees back to the office. Employers should adapt their workplaces to "earn" their employees' commute, as explained by a Deloitte.com researcher.

Cash App users can receive compensation for security breaches

Users of the mobile payment service, Cash App, may be eligible to receive a portion of a proposed class-action settlement. Early in 2024, Cash App and parent company Block Inc. were accused of "failure to exercise reasonable care" in protecting users' personal data.

Although denying any wrongdoing, the companies agreed to pay a $15 million settlement for the claim, which cited two incidents of users' account data being compromised, both of which resulted in numerous unauthorized charges on the app.

Customers affected by the breaches can submit a claim for a portion of the settlement money, which can include $2,500 in out-of-pocket losses, $25 for lost time, and additional assistance to reimburse for transaction losses.

Of the $15 million settlement, some will go to attorney fees, some to administration costs, and the remaining amount will be divided amongst impacted customers who submit eligible claims.

If you were affected by the Cash App security breaches, either through unauthorized access of your personal information or fraudulent withdrawals that occurred between August 23, 2018 and August 20, 2024, you can submit a claim on the official settlement administrator's website. The deadline to submit a claim is Nov. 18, and the final approval hearing is slated for Dec. 16.

Alternatives to MFA

Most of us already know that Multi-factor authentication (MFA) is a vital tool in safeguarding personal and organizational data from increasingly sophisticated cyber threats.

For many employees, the extra steps involved in MFA can be inconvenient and time-consuming. Also, technical difficulties, such as network issues or biometric scanner mishaps can cause MFA to fail. Some employees are also uncomfortable using their personal devices for work-related security measures.

Fortunately, there are several alternatives to standard MFA to help balance security and user convenience.

Authenticator Apps on Work Devices: Instead of using personal phones, employees can use authenticator apps on their work-provided laptops or tablets.

Biometric Authentication: Using biometric data, such as fingerprints or facial recognition eliminates the frustration of having to remember passwords.

Desktop-Based Authenticators: Applications like Authy can be installed on desktop computers, allowing users to receive authentication codes without needing to use a personal mobile phone.

Hardware Tokens: Physical devices, such as YubiKeys, that generate a code or connect to the computer via USB offer a secure and reliable alternative. They are particularly useful in environments where mobile device use is restricted.

These alternatives can help your organization enhance security, while also offering solutions to the challenges associated with traditional MFA.

By considering the specific needs and preferences of employees, managers can utilize suitable authentication methods and remain secure and compliant.

ITAD (IT Asset Disposal) Service

We have a new service, ITAD (IT Asset Disposal) that's now available. If you're interested in clearing out old IT equipment, please let us know. This is a HIPAA-compliant service.

DanTech Services clients will receive this service at a reduced rate, yet we will make this affordable to newsletter readers as well (certain restrictions apply).

What we need is a count of devices to be disposed of based on the below categories.

Once we place the order and schedule for pickup, it will be up to your team to have the equipment ready to go. Please also make sure you have an accurate list of disposed items for your records, although all we need are device counts and address for pickup.

		Desktops
—	▯	Servers
—	▮	Networking & Switches
—	▯	Hard Drives
—	▯	Monitors
—	▭	Laptops
—	▯	Tablets
—	▮	IP Phones
—	◣	Scanners
—	▯	Enter the asset type...

A team of one or more people will arrive to remove the stuff. Once finished, you'll receive a certificate of disposal.

Clean out your closets, sheds, and workspaces! Free up that valuable real estate! Contact us at info@dantechservices.com with the subject line "ITAD" and we'll get back to you.

_____

The payments will vary, depending on eligible losses and on the number of people who submit a claim. Proper documentation is required.

In addition to the settlement money they are paying, Cash App and Block agreed to work toward strengthening their data security.

As a consumer, guarding your digital identity is crucial. it's important to implement hard-to-guess passwords and to enable multifactor authentication (MFA) whenever possible to fortify your defenses. If you are notified of a breach, promptly change your password and monitor your accounts for any signs of unauthorized activity.

For businesses, it's a critical responsibility to protect your clients' data – a cornerstone of corporate trust and integrity. Safeguarding your client data is imperative to avoid financial and reputational damage, enhance customer loyalty, and maintain strong ethical standards. It's important to regularly assess and update security protocol, including the location of your sensitive data, the security of your network, your rules of accessibility, and your plan of response in case of a breach, in order to stay ahead of evolving cyber threats and technological advancements.