SIM2K
Adapting Technology to Your Business Needs

January, 2023
Information you can use

SIMformation

Tech Debt A Danger to Any Company

We all sat and watched the meltdown for air travelers over the holiday week. Southwest Airlines came to a screeching halt as it could not reconcile planes with air crews and flight cancellations. The underlying culprit for this fiasco is known as Technical Debt.

Technical debt is real debt
It's been an open secret within Southwest for some time … that the company desperately needed to modernize its scheduling systems. This problem – relying on older or deficient software that needs updating – is known as incurring technical debt. This appears to be a key factor in why Southwest Airlines couldn't return to business as usual the way other airlines did after last month's major winter storm.

When hiccups or weather events happen, the employees have to go through a burdensome, arduous process as Southwest hadn't sufficiently modernized its crew-scheduling systems. For example, if a flight was canceled, employees had to manually call in to let the company know where they were located. Many crew members reported being left on hold on the phone for hours just to let the company know their whereabouts, which led to a systemwide halt.

Such breakdowns resulting from technical debt are often triggered by external events, like weather. So why didn't Southwest simply update its software and systems? Updating software is costly and difficult. But in today's technological economy, companies cannot leave the operation of infrastructure to antiquated software. Technical debt is real debt. It will eventually be paid by someone.

Southwest's long-running reliance on a crew scheduler program called SkySolver is largely to blame. The nearly two-decade-old program was incapable of tackling the multiple waves of cancellations and delays. Southwest employees were forced to manually attempt matching flight crews with available planes.

Southwest pilots reportedly begged company executives to update the "antiquated" systems since at least 2015. Despite Southwest's previous CEO Gary Kelly praising the airline's "wonderful technology" in 2021, it has since experienced multiple logistical collapses due to its long-delayed adoption of data systems that can handle crises as large as winter storms. Until companies like Southwest actually start investing in bringing their software into the modern age, travelers can continue to expect future headaches.

Technical debt builds up because it costs money to dedicate developer time to fix the issues. So they get ignored. Every business has a problem with technical debt. Most just get lucky and don't get publicly smacked in the face with theirs like we have seen with Southwest.

Leaders underestimate the real business cost of technical debt.
Technical Debt is not unique to Southwest. Companies in all industries are hobbled by outdated, fragmented, malfunctioning, non-scalable and vulnerable IT systems. Yet, many boards overlook technical debt and miss its far-reaching business implications. While typical fixed asset borrowing is repaid with interest over time, tech debt grows silently "off the books" without any funding requirements and stealthily imperil operational excellence aims. Southwest's board and c-suite were not proactive in resolving technical debt, instituting redundancy plans and monitoring implementation progress.

There's an important lesson for all companies. Southwest routinely makes best employer rankings. Executives cannot be content with employee satisfaction alone, they must persistently uncover, assess and resolve difficult workplace issues. After all, senior leaders' fundamental stewardship obligations rests in ensuring "what must go right" as much as preventing "what could go wrong." That takes open communication.

Southwest estimates the cancellations will reduce its 2022 Q4 earnings by up to a staggering $825 million. That loss includes nearly $425 million in lost revenue and the rest in ticket refunds, expense reimbursements and overtime pay. The airline's stock is down 16% in the past month and it company valuation now stands around $20 billion, just slightly above early pandemic levels. Congressional inquiries, regulator scrutiny and class-action litigation will follow along with fines, attorney fees, time-consuming testimony and report preparation which increase the real cost of technical debt. That's a massive, additional cash flow burden.

Technical debt is the result of the design or implementation decisions you make and how those decisions age over time if they aren't incrementally adjusted or improved. The longer you hold fast to those designs and implementations without incremental adjustments or improvements, the larger the debt, or effort, becomes to make those needed changes. Our goal at SIM2K is to work with our clients to review their technology, not only from the hardware/software perspective, but how tech is embedded in day-to-day operations. We look at new IT trends and how those might apply to clients' workflow and make recommendations that we hope will be taken under advisement by our clients and reduce the onus of tech debt. Call us for more information.

LastPass Hack Still An Issue

The security mantra has been "You need to use a password manager to generate strong, unique passwords and keep track of them for you." And if you finally took the plunge with a free and mainstream option, particularly during the 2010s, it was probably LastPass. But as we reported last month, the worrying announcement that a security incident the firm had previously reported was actually a massive and concerning data breach that exposed encrypted password vaults – the crown jewels of any password manager – along with other user data. The details LastPass provided about the situation were worrying enough that security professionals quickly started calling for users to switch to other services.

LastPass has yet to clarify when the breach occurred. It seems to have been sometime after August 2022, but the timing is significant, because a big question is how long it will take attackers to start "cracking," or guessing, the keys used to encrypt the stolen password vaults. If attackers have had three or four months with the stolen data, the situation is even more urgent for impacted LastPass users than if hackers have had only a few weeks. In characterizing the scale of the situation, the company said in its announcement that hackers were "able to copy a backup of customer vault data from the encrypted storage container."

The breach also includes other customer data, including names, e-mail addresses, phone numbers, and some billing information. And LastPass has long been criticized for storing its vault data in a hybrid format where items like passwords are encrypted but other information, like URLs, are not. In this situation, the plaintext URLs in a vault could give attackers an idea of what's inside and help them to prioritize which vaults to work on cracking first. The vaults, which are protected by a user-selected master password, pose a particular problem for users seeking to protect themselves in the wake of the breach, because changing that primary password now with LastPass won't do anything to protect the vault data that's already been stolen. This means that LastPass users should go through their vaults and take extra steps to protect themselves, including changing all of their passwords.

We recommend that you start by turning on two-factor authentication for as many of your accounts as possible, particularly high-value accounts like your email, financial services, and highly used social media accounts. This way, even if attackers compromise the passwords for the accounts, they can't actually log in without the one-time code or hardware authentication key you've added as the second factor. Next, change the passwords for all of those sensitive and high-value accounts. And then change all the remaining passwords stored in your LastPass vault.

SIM2K also offers an alternative, Keeper Security. Keeper generates high-strength, random passwords and enables secure sharing among users and teams. You can create shared team folders and restrict whether users can add, remove, modify or share records. Using Keeper, IT administrators can monitor and control password use across the organization; enforce security policies and controls, such as multi-factor authentication (MFA), RBAC and least-privilege access; and monitor the dark web for passwords that have been compromised in other organizations' data breaches. As a Keeper partner, we can quickly add this to your security mix and help set up and administer Keeper for your organization. Call us for more information, especially if you have relied on LastPass for your password management.

The Met Opera Hacked

A New York City cultural institution's misfortune has a silver lining for its fans: the Metropolitan Opera sold tickets for $50 because of a cyberattack. The FBI is investigating the December attack, which took down the opera's website and box office systems, amid concerns it might have been carried out by Russian hackers because of the venue's high-profile support for Ukraine.

The $50 tickets were for general admission for upcoming performances of Rigoletto and Aida. They were the only new tickets on sale until the hack gets resolved, the venue said. The Met added that because of the hack, they do not know what seats are empty until before the performance and buyers will be directed to empty seats by ushers just before it begins.

The timing could not be worse as the Met Opera sells $200,000 tickets daily during the holidays. The Metropolitan Opera has been struggling to recover from the financial instability caused by disruptions from the pandemic. The Met reported disappointing results after just 61% of tickets sold. Across 196 staged performances, sales were down 75% from the last season before the pandemic hit in 2018-19.

"The Met has experienced a cyberattack that has temporarily impacted our network systems, which include our website, box office, and call center," it said in a statement on an emergency website "All performances will take place as scheduled; however, at this time we are unable to process new ticket orders or facilitate exchanges and refunds. We are grateful to our friends at Lincoln Center for the Performing Arts who have allowed us to continue to offer tickets to select upcoming performances through their website," they added. Even payroll operations have been affected, meaning its staff are working without knowing how and when they will get paid.

In a statement to the New York Times, Met's general manager Peter Gelb stated it would take several more days to restore the Met's ticketing site. "It takes time because when you have been hacked, you have to be sure that whatever functions are going back online are not going to be compromised," Gelb explained.

According to the Times, there is speculation that the hack is linked to Russia, potentially in retribution to the venue's support for Ukraine throughout Russia's invasion, both in producing a concert to benefit Ukrainian relief efforts and in cutting ties with Russian soprano Anna Netrebko for failing to renounce President Vladimir Putin's actions.

The Met systems were restored after a week of work, it was announced. "After suffering a cyberattack that temporarily impacted our network systems, we're pleased to announce that the Met is now able to process ticket orders through our website and in person at our box office. Based upon our ongoing investigations into the recent cyberattack, we would like to reassure our customers that ticketing customer data, including credit card information used when purchasing tickets, has not been stolen." So no institution, company or person is immune from cyberthreats, as evidenced here. Be sure your security profile is up to date.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

New Tool for Cybercrooks

The ChatGPT AI chatbot seems to have been enlisted by cybercriminals in attempts to help generate malicious code. ChatGPT is an AI-driven natural language processing tool which interacts with users in a human-like, conversational way. Among other things, it can be used to help with tasks like composing emails, essays and code.

The chatbot tool was released by artificial intelligence research laboratory OpenAI in November and has generated widespread interest and discussion over how AI is developing and how it could be used going forward. But like any other tool, in the wrong hands it could be used for nefarious purposes; and cybersecurity researchers say the users of underground hacking communities are already experimenting with how ChatGPT might be used to help facilitate cyber attacks and support malicious operations.

Threat actors with very low technical knowledge, even zero tech knowledge, could be able to create malicious tools. It could also make the day-to-day operations of sophisticated cybercriminals much more efficient and easier, like creating different parts of the infection chain.

OpenAI's terms of service specifically ban the generation of malware, and also bans attempts to create spam, as well as use cases aimed at cybercrime. However, analysis of activity in several major underground hacking forums suggests that cyber criminals are already using ChatGPT to develop malicious tools, and in some cases, is already allowing low-level cyber criminals with no development or coding skills to create malware. In one forum thread which appear towards the end of December, the poster described how they were using ChatGPT to recreate malware strains.

Researchers note that the forum user making these threads appears to be "tech-oriented" and shared the posts to show less technically capable cybercriminals how to utilize AI tools for malicious purposes, complete with examples of how it can be done. But it isn't just malware development which cyber criminals are experimenting. An underground forum member posted a thread demonstrating how they created scripts to operate an automated dark web marketplace for buying and selling stolen account details, credit card information, malware and more.

To get more information about how ChatGPT can be abused, researchers asked ChatGPT. In its answer, ChatGPT talked about using the AI technology to create convincing phishing e-mails and social media posts to trick people into giving away personal information or to click on malicious links or to create video and audio that could be used for misinformation. However, ChatGPT also defended its creation. "It is important to note that OpenAI itself is not responsible for any abuse of its technology by third parties," the chatbot said. "The company takes steps to prevent its technology from being used for malicious purposes, such as requiring users to agree to terms of service that prohibit the use of its technology for illegal or harmful purposes."

But as interest in ChatGPT and other AI tools grows, they are going to attract the attention of cyber criminals and fraudsters looking to exploit the technology to help conduct malicious campaigns at low-cost and with the least effort necessary.

"Random Tid-Bytes"

Zultys Recognized as Industry Leader

Zultys' MX System has won the 2022 Unified Communications Excellence Award. This award honors the most innovative Unified Communications products and solutions available over the past 12 months, as judged by the editors of TMC's INTERNET TELEPHONY magazine. "Congratulations to the winners of the Unified Communications Excellence Award," said Rich Tehrani, CEO, TMC. "These recipients represent the true innovators in the UC marketplace – each having proven that they deliver quality solutions to improve their customer's businesses." SIM2K is a long-standing Zultys partner and can help your business install a VoIP unified communications system. Zultys has the flexibility to be installed as an appliance at your office, or located on your own server, or even as a Cloud-based system, all offering voice, voicemail, messaging and faxing from the same system using Internet protocols. Plus, their innovative mobile app puts the same power of an office system on your smartphone. Call us for details.

Court Rules Against Ransomware Insurance Payout

The Supreme Court of Ohio issued a ruling days before the New Year that a software and service provider shouldn't be covered by insurance against a ransomware attack as it didn't cause direct or physical harm to tangible components of software, as it doesn't have any. "When insurance policy covers 'physical damage', there must be direct physical loss or physical damage of the covered media containing the computer software in order for the software to be covered under the policy," the opinion document noted. This decision overturned a lower court ruling involving EMOI Services, an Ohio-based company selling software for scheduling appointments, medical billing, and record keeping. In 2019, attackers gained access to EMOI's computer systems, planting ransomware and demanding a ransom of three Bitcoins, which amounted to $35,000 that time. After the company paid the ransom, the attackers handed over the decryption key to restore data. However, some systems and files remained encrypted, such as EMOI's telephone system and some non-critical files. When EMOI filed an insurance claim for losses from the attack – the ransom payment and costs associated with investigating the attack, remediating from it, and upgrading its security systems – Owners Insurance Co., its policy owner, denied the claim. The insurers contended the attack has no "direct physical loss to media", which is covered by the policy. EMOI then sued Owners Insurance Co, alleging breach of contract. The opinion in the Supreme Court of Ohio declared: EMOI's insurance policy is "clear and unambiguous in its requirement". "Since software is an intangible item that cannot experience direct physical loss or direct physical damage, the endorsement does not apply in this case," the ruling said, despite the policy defining computer software as a form of "media". "EMOI contends that the policy covers that damage even when there has been no damage to hardware. We are not persuaded by this argument. The most natural reading of the phrase 'direct physical loss of or damage to' is that EMOI is insured for *direct physical loss* of its media and insured for *direct physical* damage to its media," the court elaborated on its ruling. "Similarly, although the term 'computer software' is included within the definition of 'media,' it is included only insofar as the software is 'contained on covered media.' We hold that 'covered media' means media that has a physical existence." So be sure your cyberinsurance coverage is specific as to what you have covered and the language is clear. SIM2K can help define terms for you.

Fine-Tune your Android Contacts

Keeping tabs on your contacts should be about the simplest and most straightforward task imaginable in our modern connected world. But effectively wrangling your contacts on Android and keeping them manageable, organized, and optimized for efficiency really is an art. It is no wonder: Most of us have reached a point where our phones' contacts are a sprawling mishmash of clients, colleagues, college buddies, and family.

Making matters even more complex is the fact that what constitutes "Android" can be a different experience from one device to the next. The good news, though, is that it doesn't have to be so difficult.

First, if you're using a Samsung phone, experts suggest you not use Samsung's contacts, rather move to Google's better, smarter, and more platform-agnostic alternative. Here are steps to follow:

- Open up the Contacts app on your phone .
- Tap the three-line menu icon in its upper-left corner, then tap "Manage contacts" followed by "Sync contacts."
- Make sure your main Google account is present and has its toggle active on the screen that comes up next. If you don't see it, tap the "Add account" option to add it into the mix.
- Download the Google Contacts app from the Play Store. Open it up and approve the permissions it needs to operate.

If you have a non-Samsung device, check to see if your contacts app is the actual Google Contacts app or not. If not, try to find a similar set of options for syncing everything over to your Google account. If that isn't possible, find the option to export your contacts from that app and then look for the import option within the Google Contacts Android app to get to the same spot.

When you first open the Google Contacts app on Android, you'll see all of the contacts from whatever Google account is set to be the primary account on that phone. If you tap or swipe the profile picture in the app's upper-right corner, you can switch to seeing contacts associated with any other Google accounts on the device – and if you tap the three-line menu icon in the app's upper-left corner, you can shift into a merged view of all contacts from every account you've got connected.

You'll also see a list of any labels you've created for your contacts in that area. You can create as many as you like, and you can apply any number of labels onto any given contact. Labels are a good way to break that jumble of names into specific, meaningful groups.

For instance, you might have a label called "Work" that includes all employees, another called "Team" that shows only the people you directly work with, another label for clients and so on. Once you do that initial organization, you'll have an easy way to limit your view to only the individuals you need at any given moment.

To apply a label onto a contact once you've created it:

- Press and hold the name of the person from the main contact list.
- If you want to add other people to the same label at the same time, tap their names next.
- Once you have got all the names you need highlighted, tap the three-dot icon in the app's upper-right corner and select "Add to label" followed by whatever label you want.

When you first tap a person's name within the Google Contacts app, you'll see a screen with their profile. Tap the pencil-shaped editing icon in the upper-right corner of that area where you can add additional information. For example, you can tap a plain-text "More fields" link at the very bottom of the profile editing interface to reveal a whole host of other potentially useful options – including fields for nicknames, their company name, department name, work title, and even a series of people related to that person that you might need to remember (spouse, assistant, manager, or the person who referred them to you, just to name a few available options).

After tapping that "More fields" option, you'll see a new option at the bottom of the screen to add your own custom field. That's a handy way to store any additional manner of info about a person that might be helpful to find later.

If you tap the circular icon at the very top of the profile editing interface, you can upload a photo to represent the contact in question. One more advanced Android contacts option worth mentioning: When you open any person's profile in the Contacts app on your phone, you'll see a hollow star in the upper-right corner of the screen. You can tap that to fill the star in and mark that person as a favorite. Doing so will have some significant effects:

- That person will always appear at the top of your contacts list.
- They'll also typically show up in a special, more prominent area of your Phone app for extra-easy access.
- And they'll be granted special privileges to reach you even when your phone is in Do Not Disturb mode, with the specifics depending on your preferences in that area of your system settings.

Now you can optimize your contacts. From the Contacts app on your phone, tap "Fix & Manage" at the bottom of the screen – then tap the "Merge & Fix" button. Look to see what suggestions the app gives you, then tap them and follow the steps presented.

Once you've gotten your contacts created, organized, and cleaned up properly, the Google Contacts app on Android has several advanced actions that are all too easy to miss.

You can use the Contacts app as an efficient way to start a new group e-mail or text message thread with any selection of people you want. Just make sure the people are all in the same label, then tap the three-line menu icon in the app's upper-left corner and select the label. Next, tap the three-dot menu icon in the upper-right corner of the label screen and look for "Send e-mail" or "Send message."

The Contacts app can also serve as an all-in-one hub for initiating communication with anyone in your collection. Open someone's profile, and you'll see one-tap icons for calling them, texting them, e-mailing them, or starting a Google Meet video call with them.

For easier access to high-profile people, use the Google Contacts widget options: Long-press on any open area of your home screen, select the option to add a widget, and then look for the Contacts section. There, you should see an icon to add a new overall contact shortcut as well as an icon to add a one-tap command for calling or texting any particular person. You can add as many of those as you want onto your home screen.

Last but not least, the real beauty of the Google Contacts setup on Android: It works equally well no matter what type of device you're using. And to move to a new device, simply install the Google Contacts app and all your data will instantly be there, synced, and available to you – no restoring required.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com