SIM2K
Adapting Technology to Your Business Needs

12•22
Information you can use

SIMformation

Happy Holidays from SIM2K

From all of us at SIM2K, we would like to wish you the best of the holidays. We hope that we are now past the worst of the pandemic as many companies have moved to fully return employees to the traditional office, while some still allow "work at home" to continue. We are seeing increased use of conferencing products as companies have recognized the utility of these tools. Scammers are still taking advantage of these unsettled times and ramping up ransomware attacks on major institutions across the world. SIM2K continues to add to our product lines in Endpoint Protection, Wi-Fi, security cameras, VOIP Phones and even print management software services. As we say every year, we appreciate the loyalty of our clients and strive to continue to be your IT provider. We look forward to serving you in the year ahead!

Ben FRED CHRIS Christy Vanett Charlie Beverly Scott Justin

In memoriam - Mark Finegan

Trends for 2023

For many years now SIMformation has taken a look at the "crystal ball" of technology to help prepare for the upcoming new year. Businesses need to know what is coming to adequately prepare for navigating new technology that has never been more challenging to assess. Perhaps the most crucial step to ensure your business is positioned for near-term success is to familiarize yourself with the top tech predicted for 2023. After all, if you haven't begun to equip your organization for the year's top tech advances once the new year arrives, you'll be late to the dance!

Given that, here are some of 2023's key tech trends, according to Gartner Research:

1. Digital Immune System

The past few years have seen an unparalleled focus on risk, both in the physical and digital world. Cybersecurity concerns are increasingly acute, as data breaches and other cybersecurity concerns are becoming increasingly sophisticated.

Fortunately, methods for protecting against online criminals, spammers and other "bad guys" are improving in sophistication. Through observation, automation and the latest developments in design, a robust digital immune system can significantly mitigate operational and security risks.

As the utility of these tools becomes more established, expect to hear many more questions about the health of your organization's digital immune system in the year to come, and what you're doing to strengthen and protect it.

2. Applied Observability

The 2010s saw an abundance of tools and methods of capturing more data than anyone knew what to do with. Thus, with seemingly endless quantities of client data now available, it's likely that the next step will be toward creating new uses for data that's been collected.

Applied Observability uses Artificial Intelligence to analyze and make recommendations for greater efficiency and accuracy based on an organization's compiled data. It optimizes data implementation by placing more value on use of the right data at the right time for rapid response based on confirmed stakeholder actions, rather than intentions. This can lead to real-time operational improvement, and a tangible competitive advantage for your business.

3. AI Trust, Risk and Security Management (AI TRiSM)

We've all heard a lot about AI over the past several years, but believe it or not, many industries are still in the early stages of AI implementation.

continued on page 2

2023 Trends *(con't)*

With the focus on risk throughout every industry post-pandemic, it's no surprise that AI Trust, Risk and Security Management (AI TRiSM) will be a major focal point in the tech space next year. AI TRiSM combines methods for explaining AI results, new models for active management of AI security, and controls for privacy and ethics issues, all in support of an organization's governance, reliability, security, and overall health.

4. Industry Cloud Platforms

Cloud adoption has been a major component of digital transformation for over a decade, and 2023 will almost certainly prove to be another year for more sophisticated, industry and organization-specific cloud adoption strategies. By combining SaaS, PaaS and IaaS with customized functionality, Industry Cloud Platforms may prove to be the most consequential step toward cloud adoption to date.

5. Platform Engineering

As adoption grows and digital platforms mature, expect to see an increased emphasis on customization. That's what platform engineering offers: a set of tools and capabilities that are developed and packed for ease-of-use. For development teams and end-users alike, this could mean increased productivity and simplified processes.

6. Wireless-Value Realization

We're still only beginning to scratch the surface of the value gained by the integration of wireless technology through a broad, interconnected ecosystem.

In the coming years, we'll see wireless endpoints that are able to sense, e-charge, locate and track people and things far behind traditional endpoint communication capabilities. Another step towards optimization of collected data, wireless-value realization networks provide real-time analytics and insights, as well as allowing systems to directly harvest network energy.

7. Superapps

Combining the features of an app, a platform and a digital ecosystem within a single application, superapps offer a platform from which third parties can develop and publish their own miniapps. An end user can activate micro or minapps within the superapp, allowing for a more personalized app experience.

8. Adaptive AI

Using real-time feedback to new data and goals, adaptive AI allows for quick adaptation to the constantly evolving needs of the real-world business landscape. The value provided by adaptive AI is apparent, but implementing these systems requires automated decision-making systems to be fully reengineered, which will have a dramatic impact on process architecture for many companies.

9. Metaverse

As noted above, you're likely familiar with the term "metaverse" by now thanks to Mark Zuckerberg. However, if the lackluster performance of Meta's stock is any indication, you're one of the many who has yet to be sold on the benefits of the metaverse.

Regardless, metaverse technologies that allow for digital replication or enhancement of activities traditionally done in the physical world should certainly not be dismissed. There is far too much at stake, and the possibilities are far too intriguing for too many people to write off metaverse technologies quite yet, even if the pilot versions fail to impress.

10. Sustainable Technology

Until recently, the tech world has been single-mindedly fixated on boosting the power of new technologies. But as tech becomes increasingly integrated into every facet of our lives, we're seeing new investments in energy efficient tech and tech that promotes sustainable practices.

Emissions management software and AI, traceability and analytics for energy efficiency are all allowing both developers to build sustainability-focused tech, and allowing business leaders to explore new markets and opportunities for sustainable growth.

As you look ahead to 2023, what challenges does your company face? Maybe your business needs to save costs, to improve margin or to reinvest. Or maybe your enterprise is still trying to grow. Perhaps this is the time for a pivot — to reinvent the business model. Some of you may even need to do all of these at once.

Gartner publishes this annual list so that business leaders and technologists can use it to assess the potential impact of these technology trends on specific strategies, such as growing revenue, accelerating digital, maximizing value from data, or protecting and building a brand. These trends could represent a risk or opportunity for your organization and this list could help you create a technology roadmap to drive impact on a range of strategic ambitions.

By looking at when these trends will become most relevant, you can establish your own pathway, realizing they also don't need to be done all at once. SIM2K can help you assess your current technology position and what steps you should consider in light of 2023 trends. Of course, this list is not exclusive of things to come, as the IT world remains in constant state of re-invention as new threats emerge, new breakthroughs in technology come on-line and we learn more on how to harness IT to be a useful, day-to-day tool. The pivot to remote work during the COVID pandemic is one example of a sudden change in IT deliverables, as companies rushed to add VPN access, collaboration tools like Zoom or Teams, and increased security for those connecting remotely. And, there is increased adoption of the 2022 advancements like 5G cellular service, Wi-Fi 6 and Gig broadband availability that are shaping how work gets done.

It's always a roller-coaster ride in technology, and be assured that SIM2K is constantly learning and assessing developments to be proactive in delivering world-class support to your business. Call us to discuss your needs, concerns and where you hope to grow in 2023.

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.

LastPass Hacked ... Again

Password management app LastPass says it is investigating a security incident after an "unauthorized party" compromised its systems and gained access to some customer information.

The information was stored in a third-party cloud service shared by LastPass and parent company GoTo, said LastPass CEO Karim Toubba, noting the hackers used information stolen from LastPass' systems in a separate previously disclosed incident that occurred in August of this year. Toubba added that "customers' passwords remain safely encrypted."

According to a blog post dated August 22, the previous incident saw a threat actor gain access to the LastPass Development environment using a developer's compromised endpoint to steal source code and some proprietary LastPass technical information. LastPass said at the time that its systems "prevented the threat actor from accessing any customer data or encrypted password vaults."

LastPass is currently working to understand the scope of Wednesday's incident and identify what specific information has been accessed. GoTo, formerly LogMeIn, said it was also investigating the incident, although it did not explain whether GoTo users were also impacted by the hack. In the meantime, LastPass products and services remain "fully functional," said Toubba.

"Given the vast amount of passwords it protects globally, LastPass remains a big target," a researcher at Silverfort said. "The company has admitted the threat actor gained access using information obtained in the previous compromise. Exactly what this information is remains unclear, but typically, it's best practice after suffering a breach for the organization to generate new access keys and replace other compromised credentials. This ensures things like cloud storage and backup access keys cannot be reused."

This isn't the first time LastPass has had security problems. In 2021, it appeared that some users' LastPass Master Passwords may have been revealed. LastPass replied that it hadn't been breached, but users who had gotten e-mails warning them that an unknown person was trying to log into their accounts weren't convinced. Nevertheless, LastPass insisted that it was just the result of a credential stuffing attack.

In 2020, LastPass had a major outage, and users reported they couldn't log into their accounts or autofill passwords. In 2019, a significant LastPass security problem was uncovered by security researchers as well.

That said, it is still concerning that the biggest password security company – with a claimed 20 million customers – has significant, annual security problems. In this case, however, LastPass has "engaged a leading cybersecurity and forensics firm" to investigate what happened. LastPass is also implementing enhanced security measures. They've seen "no further evidence of unauthorized activity."

However, many security experts feel that this is too little, too late. But it's still something. LastPass, with its zero-knowledge model, is still a good password security company. But if you want to look for another password manager, no one would blame you.

"Random Tid-Bytes"

FBI Finally Reacts to TikTok Concerns

The head of the FBI says the bureau has "national security concerns" about the U.S. operations of TikTok, warning that the Chinese government could potentially use the popular video-sharing app to influence American users or control their devices. The FBI has "a number of concerns," director Christopher Wray told a House Homeland Security Committee hearing about worldwide threats, just days after Republican lawmakers introduced a bill that would ban the app nationwide."They include the possibility that the Chinese government could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations if they so chose, or to control software on millions of devices, which gives it an opportunity to potentially technically compromise personal devices," Wray said. TikTok, which hit 1 billion monthly active users in September 2021, is owned by the Chinese company ByteDance. Chinese national security laws can compel foreign and domestic firms operating within the country to share their data with the government upon request, and there are concerns about China's ruling Communist Party using this broad authority to gather sensitive intellectual property, proprietary commercial secrets and personal data. As previously discussed in SIMformation, the possibility of TikTok harvesting data on US citizens has been known in the IT ranks for some time, and it appears that the Biden Administration is finally taking notice of these dangers.

Biometrics May Not Be the Answer

In independent testing, many biometrics simply do not accurately deliver on their promise. On top of that, many vendors, including Apple (iOS) and Google (Android), make marketing choices in their settings, where they choose how stringent or lenient the authentication is. They do not want a lot of people being improperly locked out of their phones, so they choose to make it less strict, in effect giving a greenlight to device access by higher numbers of unauthorized people. Another key factor is theoretical accuracy versus real-world accuracy. Consider two popular phone authentication methods: facial and fingerprint recognition. In theory, facial recognition is much more discerning because it can consider a larger number of datapoints. In practice, though, that often doesn't happen. There is also a distance issue. With facial recognition, a device needs to be a precise distance from the face to read it accurately – not too close, not too far. The problem here is one of perception and characterization. These biometric efforts, as currently implemented, are little more than convenience. But they're offered as being tailored for cybersecurity. And as a result, users and technologists rely on biometrics as a protective measure. There are plenty of ways of deploying biometrics securely. Retina scans are usually secure and fingerprints work well for people that have properly scannable fingerprints. But voice biometrics, currently used by a variety of financial institutions, remain too easy to fake. This brings us back to settings decisions. If the settings are sufficiently strict, even facial recognition can become a security mechanism. In short, biometrics is a fine convenience, but as a security defense, most of today's implementations are not a panacea for cybersecurity.

Rackspace Hit with Huge Outage

Rackspace hosted Exchange suffered a catastrophic outage beginning December 2, 2022 and is was still ongoing as of the release of this issue of SIMformation. Initially described as connectivity and login issues, the guidance was eventually updated to announce that they were dealing with a security incident. Rackspace has not offered any explanation of the "security incident" that has taken out its hosted Exchange environment and led the company to predict multiple days of downtime before restoration.

Finally, on December 6, Rackspace confirmed a Hosted Exchange ransomware attack has knocked out e-mail service to customers. The attack "may result in a loss of revenue for the Hosted Exchange business, which generates approximately $30 million of annual revenue," Rackspace disclosed — four days after the ransomware attack occurred.

Rackspace ($RXT) has hired "world-class external expertise" to assist with the security incident investigation, the company said, though specific MSSP and incident response company names were not disclosed. The incident started early on December 2. As this issue has continued, Rackspace still has not announced an ETA for Hosted Exchange system recovery.

In response to media inquiries, Rackspace said its incident status page and an FAQ provided to customers are all it can provide at this time. Both documents warn of a lengthy outage, and advise migration to Microsoft 365 for mail services. Both are also silent on the risk of data loss, or data leaks.

Many social media reports mention not being able to restore all inboxes after migration. And given that email is used to store way too many documents, the risk of leaks is very significant.

The status page has at least been updated regularly. While it assures that Rackspace has restored "thousands of customers," it's unclear whether those thousands represent the bulk of affected users or a tiny minority. And for the rest, the news remains grim.

When the hosted Exchange service became unavailable, Rackspace quickly advised of – and offered free access to – Microsoft 365 as the fastest way to restore service, and offered do-it-yourself instructions on how to make the move.

Despite Rackspace's advice that the migration procedure should take between 30 and 60 minutes, some users found that option was not simple to implement. Customers who profess to having little technical expertise – which is fair enough given Rackspace promotes its hosted Exchange service as suitable for "any business size or need" and that an "award-winning team of support experts is available to solve your technical problems 24x7x365" have found it hard to implement the instructions. Worse, customers of all sizes have also found the promise of swift support is not currently being fulfilled.

Here is what Rackspace is asking customers to do:

> *Your account administrator will need to manually set up each individual user on your account. Once your users have been set up and all appropriate DNS records are configured, their email access will be reactivated, and they will start receiving emails and can send emails. Please note, that DNS changes take approximately 30 minutes to provision and in rare cases can take up to 24 hours.*
>
> *IMPORTANT: If you utilize a hybrid Hosted environment (Rackspace Email and Exchange on a single domain) then you will be required to move all mailboxes (Rackspace Email and Exchange) to M365 for mail flow to work properly. To preserve your data, it is critical that you do not delete your original mailboxes when making this change.*
>
> *Self-migrating can be challenging so if you need assistance, please leverage our support channels by either joining us in chat or by calling +1 (855) 348-9064.*
>
> *You can also implement a temporary forwarding that will allow mail destined for a Hosted Exchange user to be routed to an external email address. Please log in to your customer account for a ticket with instructions to request this option. Customers should reply to the ticket to request the forwarding rule be put into place for each of their users.*
>
> *If you do not see this ticket in your account and would like to take advantage of this option, please open a support ticket with the title: REQUESTING FORWARDING FOR HOSTED EXCHANGE. We will work with you to get this setup.*
>
> *NEW mail that is sent after the forwarding rule is put in place will be forwarded to the external address specified.*
>
> *The forwarding rule will not apply retroactively to mail sent before the rule is put into place. This option can be used as a temporary solution while you set up Microsoft 365.*
>
> *Once you have fully set up Microsoft 365 and updated your DNS MX records, this forwarding rule will no longer be needed.*

This is not the sort of "fix" that is easily done, and indirectly acknowledges that some mail may be lost during the shift to forwarding or over to M365. So while a fix, it is not perfect and any customer should be aware of this fact.

Rackspace's recent updates state that it has thrown 1,000 of its staff into support duties in an attempt to address "much longer than usual" wait times. But angry customers have sent social media posts about being left on hold for four hours.

> *"This is a pathetic response," tweeted one user. "That reply is not acceptable to those impacted," read another reaction.*
>
> *"Unbelievable," read one tweet. "After 5 hours on hold, call was answered, we gave info politely, agent said to hold on a moment, and we were disconnected. Poof. No help, wasted time."*

Details remain to be seen about any security posture from Rackspace that may have led to the problem. However, partners have pointed to systemic failings. "Just from the standpoint of them not being able to get the systems back up in a reasonable amount of time and running shows there is some type of failure in their disaster recovery process. Was this a new sophisticated attack or were their servers left unpatched? We just don't know yet," one Rackspace MSP commented.

This attack underscores the need for security vigilance for any company. A major player in the IT world can be crippled by ransomware just like a small business. SIM2K offers training to help employees identify potential threats, and has endpoint security products to further help fortify your company's security profile to help protect you. Call us for more information.

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

Attacks via Facebook

Multiple restaurants in Cincinnati are fighting cyber hackers who have stolen thousands of dollars, damaged reputations and shut down social media sites. “When it happened, it was instant panic,” said Arnold’s owner Chris Breeden. “Facebook is basically the most important advertising tool we have in our tool bag, and it’s pretty devastating when you lose something like that.”

Breeden said the thieves hacked into one of their social media accounts and then got into their Facebook site. Once there, they were able to tap into bank accounts associated with Arnold’s Facebook.

The thieves bought ads, turning money from bank accounts into Facebook advertising currency to be used in other countries.

To ensure Arnold’s couldn’t get back into their social media accounts, the hackers posted severely inappropriate material that got Arnold’s account banned for life.

“I'm like super banned. I couldn't be more banned since they posted explicit material. It triggers an auto ban. So, that auto ban hit me. Then, it blocked me from getting my business page, then it blocked my personal Instagram and Arnold's business into Instagram. So, we have been completely shut out of all social media,” Breeden said.

Crown Restaurant Group reported similar attacks at four of their restaurants.

In recent months, Thomas More University was locked out of its Facebook account.

“I think it’s increasingly common,” said a cybersecurity expert. “Your account’s taken over, you’ve lost all those followers, you’ve got to try to rebuild that, and just the time and money it costs to recover from something like this.”

This should be a wake-up call for other small businesses to strengthen passwords and take cyber security seriously. Fixing the problem can take months or longer if it can be fixed at all. You can’t just pick up the phone and call someone and say, ‘Hey, I’m restaurant XYZ, can you unlock my account for me?’ Unfortunately, it doesn’t work that way. Damage from on-line trolls and now even direct compromise of social media sites can quickly destroy a company’s reputation, and can take months to overcome, if they even their reputation can be resurrected. So take pains to safeguard your social media accounts, be it Facebook, Instagram, Snapchat or, help us, TikTok. The “bad guys” are always looking for some inroad to capture information they can use to hack deeper into your company information, banking and other data, no matter what size your business might be.

More TikTok Bad News

A TikTok challenge has been jumped on by cybercriminals, who are taking advantage of its popularity to try to trick people into downloading malware that steals their information.

The Invisible Challenge sees people use a filter to make their body appear see-through, leaving just the silhouette visible. Some people are using the filter and then taking their clothes off on screen. They’re naked, but the user doesn’t see that because they are “invisible”.

Naturally, that’s left some people wondering if they can remove the filter, after posting, in order to see the person actually naked.

Enter the scammers. According to researchers at Checkmarx, attackers posted online that they had created an app that was able to remove the invisible body filter. All interested parties need to do is join the Discord server discord.gg/unfilter to get the app.

Once they joining the Discord server, they are shown videos that supposedly show the results of the filter removing software. However, instead of installing the app, what they actually get is a WASP information stealer, which searches the infected device for passwords, cryptowallets, credit cards, Discord accounts, and any other files that might be interesting, and sends all of it to the attacker.

Then they’ll receive a private message from a bot account asking them to give a star to the GitHub repository. The repository had at least 103 stars which may be a good indicator for the number of victims that installed the stealer. Ever since the discovery, several elements of the attack have been reported and removed, but it doesn’t seem like the attackers are ready to give up on this profitable project. So, whatever you do, don’t follow up on the claims that the invisible filter can be removed. Also, if someone has used an invisible filter, its because they don't want you to see the “invisible” portion, so don’t try to find a workaround.

If you’re using the filter yourself, it also works if you keep your clothes on. That way, if anyone actually finds a way to remove the filter, you won’t have caught yourself on camera.

Better yet, stay away from TikTok altogether. The number of reports about personal information being exposed from this app make it highly suspect, as we have and continue to cover in SIMformation.

If you think you’ve been infected with the information stealer yourself, you should change the passwords that were stored in your browsers. Also change or add 2FA to your online accounts wherever you can, and keep an eye on your bank and credit card statements.