SIM2K
Adapting Technology to Your Business Needs

12•21
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. Technology continued to cope with the pandemic as many companies have yet to fully return employees to the traditional office and allowing "work at home" to continue. Cloud-based applications are seeing growth, too, to support the distributed workforce. Scammers are taking advantage of these unsettled times and ramping up ransomware attacks on major institutions across the world, many believed to be state-sponsored from China, Iran and Russia. SIM2K continues to add to our product lines in 2FA (two-factor authentication), 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 Christy Nick Chris JOHN Scott

In memoriam - Mark Finegan

Trends for 2022

We saw how 2020 upended life and business as we know it. Then, 2021 was spent picking up the pieces of what the pandemic left behind. It wasn't back to life as usual, however, as organizations and workers found that many pre-pandemic systems would never be the same again.

Looking ahead to 2022, there are a variety of trends that have come about as a result of the pandemic, and some that have stayed around because of it. Included in these is remote work, cloud usage, and new cybersecurity measures.

We have gazed into the IT crystal ball to put together some of the top technology trends of 2022 that are sure to be on the top of industry priority lists.

Hyperautomation was one of the top trends of 2021. What continues to change about hyperautomation is its adoption and evolution. There has been tremendous demand for automating repetitive manual processes and tasks, so robotic process automation was the star technology that companies were focused on to do that. Now it has moved from task-based automation to process-based automation, to functional automation across multiple processes and even moving towards automation at the business ecosystem level. Hyperautomation in 2022 will combine technologies like Robotic Process Automation (RPA), Artificial Intelligence (AI), and Machine Learning (ML) to process information to improve quality, increase overall productivity, and offer real-time, continuous intelligence with improved analytics to further enhance operations and processes.

Anywhere Operations. During the height of the pandemic it was estimated some 2/3 of employees were working from home. Although these numbers are decreasing, there is still a large percentage of employees working out of the office. Companies need to incorporate technologies that enable seamless collaboration regardless of location. Anywhere operations refers to an IT operating model that:

- Enables employees to work from anywhere
- Supports the deployment of business services across a distributed infrastructure
- Works well with mobile devices, which is highly beneficial to customers

Whether services need to be available on a desktop computer, tablet, mobile phone or other device, companies are beginning to catch on in the services they must adopt or offer.

continued on page 2

Trends *(con't)*

The opportunities are endless, ranging from intelligent cameras and collaboration systems equipped with AI for conference calls to entire platforms of software and infrastructure ecosystems that provide teams a digital headquarters.

5G. The demand for high-speed internet and smart home and city systems has pushed the development and adoption of 5G technologies for organizations. In 2022, large enterprises as well as small start-ups will begin to create innovative infrastructures and applications in order to:

- Increase employee productivity
- Transform the customer experience
- Create new jobs
- Support mission-critical communications
- Provide massive IoT opportunities

5G is quickly becoming the network of choice largely due to its reliability and performance. The Global 5G Infrastructure Market size was valued at $1179.2 million in 2021 and is expected to reach $131.40 billion by 2030.

Hybrid Cloud. Simply using the "Cloud" is no longer enough. Businesses must evolve and utilize different types of clouds in order to gain the most benefits from it. 2022 will be the year of the hybrid cloud, with vendors competing for the perfect mix of public and private clouds as organizations face challenges of data access and security. A recent survey found that teams who used hybrid or multi-cloud software deployments were 1.6 times more likely to meet their organizational performance targets than those who used more traditional cloud strategies.

Companies that turn to more than one public cloud for solving business needs and challenges will become the norm, and as the year progresses it might even become a necessity. With data being created exponentially faster than ever before, and at the edge, this will only push the need to migrate.

Privacy-Enhancing Computation. As legislation for global data protection matures, privacy will become increasingly important, furthering the need for privacy-enhancing computation which will protect data in use while also maintaining its privacy and secrecy. This will be critical in Multi-party data analytics use cases and untrusted environments.

Consumers are starting to notice. With the massive amounts of data users volunteer to apps and social media sites, questions are being raised as to what happens to this data and why it is being collected. Organizations will need to find new sources of data and be honest in its management in order to obtain the same level of customer experience.

Artificial Intelligence Engineering. Each day, the world creates roughly 2.5 quintillion bytes of data, and that number is only continuing to increase at an exponential rate. However, the use of that data is only as good as the systems put in place to manage, regulate, and evaluate it. This enormous task is nearly impossible to be performed manually by workers, so companies have been turning to artificial intelligence (AI).

AI engineering is about providing a sort of engineering discipline that will emphasize having AI projects that are delivered in a consistent way to ensure that they can scale and move into production. It is bringing the engineering discipline to AI for end-user organizations. This robust strategy will:

- Help projects reach development
- Improve the scalability, performance, and reliability of AI models in general
- Increase ROI

Cybersecurity Mesh. With more employees working remotely and the cloud becoming the norm, businesses are looking for new approaches to their network security. A mechanism that will be seen more often this upcoming year is cybersecurity mesh.

Cybersecurity mesh is a distributed architectural approach that provides flexibility, scalability, and reliability to cyber controls. Cybersecurity mesh essentially allows businesses to decouple policy decision making from policy enforcement: a cybersecurity mesh puts security perimeters around individuals – instead of just around the organization. Utilizing this mesh technology, organizations will be better able to protect data and information, including what's inside the facility walls, as well as everything that's on the outside.

Edge Computing is closely tied to the Internet of Things (I0T). It connects a variety of devices to bring users a mix of services and products that are more customizable and personal. Companies can expect edge computing to improve:

- Predictive maintenance
- Fleet and product management
- Voice assistance

So what do we expect in 2022? COVID-19 will continue to impact the way companies do business, and the way employees work. As we see accelerated uses of digitization and virtualization, the need for cloud, security, privacy, and automation will increase. True transformation is possible, and these trends will push many businesses forward into the future of tech. SIM2K continues to adapt our business practices and offerings to reflect these changing times, and to introduce these new technologies to our customer base. If you look at the tremendous changes in IT over the past decade, the growth has been more than exponential so staying abreast of these changes is challenging.

But, we can't let those that exploit technology for ill-gotten gains outpace us. That's why these trends are important, even if your company may not need some of the more advanced tools. But as we have seen, these trends eventually trickle down into everyday tech offerings, so we feel it is important for you to know what is coming down the pike and be comfortable with where tech will head in the next year and beyond.

We are always open to meeting with you to assess your tech platform and offer counsel on how to address any needs now and for the future. Please call us for more information on our CIO services.

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.

Microsoft Boosts Security Workers

Microsoft will partner with community colleges across the U.S. and provide free resources in an attempt to help end a shortage of cybersecurity workers, the company has announced. The company believes it can reduce the country's workforce shortage by half by 2025. It aims to help train and recruit 250,000 people into the cybersecurity workforce by then.

"We think we can make a meaningful difference in solving half of the cybersecurity jobs shortage," Microsoft President Brad Smith said in a press conference, adding that "we should be optimistic that in the next 12-24 months we can start to make a real dent."

The company announced it will provide a free curriculum to community colleges across the country, provide training for faculty at 150 community colleges and give scholarships and resources to 25,000 students as part of the effort.

Smith said data compiled by Microsoft shows that there is one open cybersecurity job for roughly every two that are filled in the U.S. And of all available positions in the U.S., more than one in 20 is a job requiring cybersecurity skills. Microsoft said such jobs pay an average of $105,800 per year and can range from chief information security officer roles to those requiring a mix of IT and cybersecurity know-how.

In addition to addressing the workforce shortage, Smith said the campaign will play an important role in diversifying the industry. Microsoft found that men hold 82.4% of cybersecurity jobs in the U.S. and 80% of those jobs are held by people who are white. According to data compiled by Microsoft, 57% of community college students in the U.S are women and 40% of students identify as Black, African American or Hispanic.

According to data cited by Microsoft, there are 464,200 open jobs in the country that require cybersecurity skills, or 6% of all open jobs in the country, with average annual pay of $105,800.

The announcement follows commitments Microsoft made after a White House cybersecurity summit in August with President Joe Biden and CEOs across several industries. Microsoft said at the time it would spend $20 billion over five years to deliver more advanced security tools and invest $150 million to help government agencies update their security systems and expand training partnerships in cybersecurity.

Several high-profile cyberattacks have drawn public attention to the potential risks associated with cybercrime. An attack on government software contractor SolarWinds revealed last year affected several federal agencies, for example, and a separate attack on Colonial Pipeline caused a major gas shortage in the Southeast. Flaws in Microsoft's widely used software and cloud services also contribute to the nation's challenge, as evidenced this year by a major Microsoft Azure database vulnerability, and high-profile Exchange Server hack.

Both the private sector and government officials have pointed to the workforce shortage as a persistent problem as they try to take on such breaches.

Microsoft is working on the cybersecurity skills initiative with organizations including the American Association of Community Colleges, the Last Mile Education Fund, and Whatcom Community College, Bellingham, Wash., home to the National Cybersecurity Training & Education Center.

"Random Tid-Bytes"

Iran Wants Into the Act

In November, the CISA, the FBI, the United Kingdom National Cyber Security Centre (NCSC), and the Australian Cyber Security Centre (ACSC) released a Joint Cybersecurity Advisory, "Iranian State-Sponsored advanced persistent threat (APT) Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities." The Iranian government-sponsored APT actors are actively targeting a broad range of victims, affecting multiple critical infrastructure sectors, including the Transportation Sector and the Healthcare and Public Health Sector. FBI, NCSC, ACSC, and CISA assess the actors are focused on exploiting known vulnerabilities rather than targeting specific sectors. Access gained by these Iranian Government-sponsored APT actors can be leveraged for follow-on operations such as data exfiltration or encryption, ransomware, and extortion. The advisory provides indicators of compromise (IOCs) that are likely associated with this Iranian government-sponsored APT activity. So again, another state-sponsored hack attack is presented, so maintaining vigilance against malware and threats is imperative.

Navy Ship's Facebook Page Hacked

The official Facebook page of the US Navy's destroyer-class warship, USS Kidd, has been hijacked. According to reports on the incident, the account has done nothing but stream Age of Empires, an award-winning, history-based real-time strategy (RTS) video game wherein players get to grow civilizations by progressing them from one historical time frame to another. In an interview, a Navy spokesperson confirmed the hijacking: "The official Facebook page for USS Kidd (DDG 100) was hacked. We are currently working with Facebook technical support to resolve the issue." The hijacked account started streaming the video game live on October 4 for four hours. That session was followed by five more streams one after the other, each lasting for up to two hours. Official accounts of the US military getting compromised is rare but not unheard of. A year ago, the administrator responsible for the Fort Bragg Twitter account forgot to switch from that account to his own personal Twitter account before posting lewd comments on a model's page.

AdBlocker Actually Injects Ads

Researchers have uncovered a new ad injection campaign based on an adblocker named AllBlock. The AllBlock extension was available for Chrome and Opera in the respective web stores. The extension replaces all the URLs on the site a user is visiting with URLs that lead to an affiliate. This technique means that when the user clicks on any of the modified links on the webpage, they will be redirected to an affiliate link. Via this affiliate fraud, the attacker earns money when specific actions like registration or sale of the product take place. To make the extension look legitimate, the developers actually implemented ad blocking functionality. Further, the code was not obfuscated and nothing immediately screams malware. All the URLs that are present in a visited website are sent to a remote server. This server replies with a set of replacement URLs which the extension then give permission to do so. So be aware of this compromised adblocker and do not install it.

MultiFactor Authentication May Be At Risk

Every time a massive data breach makes the news, we remind you about the best practices you need to employ to protect your online properties. You should never use weak passwords and recycle them. Instead, pick a password manager that lets you generate unique passwords for every different service, website, and app. And use two-factor authentication (2FA) or one-time passwords (OTP) whenever you can. That way, when hackers inevitably hack one of your accounts, your other properties are protected. But you should remain vigilant when it comes to defending your online accounts.

Unfortunately, the tech world is finding out that unique passwords and 2FA/OPT aren't enough, as hackers have found a clever way to trick you into giving them that unique code they need to break into your account. And you might not even realize that you've opened the doors to your Amazon, PayPal, Coinbase, or bank account to attackers who might steal money from you. It's all possible thanks to a new type of customizable bots that place automated calls with the sole scope of stealing that temporary password.

Even without bots, 2FA protection isn't foolproof. Some hackers might try social engineer attacks to convince you to give up that temporary code or password. But not all of them might be that convincing. On the other hand, the bot is a lot more sophisticated and will make you believe that you're talking to the automated security system belonging to the service that hackers want to penetrate. A security company demonstrated the attack with a simple example, an incoming call supposedly coming from PayPal's fraud prevention system.

An automated voice tells the PayPal account holder that someone tried to spend a particular sum of money. PayPal needs to verify the account holder's identity to block the transfer, and they'll ask for the 2FA/OTP.

The bot sounds just like one of the bots you're might be talking to during regular customer service calls. They'll invite you to press certain keys and then to input your 2FA/OTP code. But as soon as you do, the code reaches the hacker who initiated the attack.

The company played a recording a hacker used to implement this scam:

> 'In order to secure your account, please enter the code we have sent your mobile device now,' the voice said. PayPal sometimes texts users a code in order to protect their account. After entering a string of six digits, the voice said, 'Thank you, your account has been secured and this request has been blocked.'

The bot then proceeded to inform the user there's no reason to worry about:

> 'Don't worry if any payment has been charged to your account: we will refund it within 24 to 48 hours. Your reference ID is 1549926. You may now hang up,' the voice said.

Hackers who obtained someone's personal data – such as their real name, email address, and phone number – might use it to determine whether they have a PayPal account with that address. They can apply the same procedure to any sort of online account. Once they find a match, they can feed the victim's phone number to a bot that's tailored for that service.

The security firm explained that these bots can cost a few hundreds of dollars per month and target specific services like Amazon and PayPal. Others can target specific banks like Bank of America and Chase. And some of them let you customize the experience to any type of account.

The reason you get a code via text message on your phone is that the hacker has tried to log into your account, fully knowing they won't be able to get into it. The bot makes it sound that it's a service like PayPal that's generating the unique 2FA/OTP code. And you'll have no way of knowing it's a hacker targeting you. Especially as you rush to deal with the threat. Once inside your account, the hackers can steal money or cryptocurrency.

Next time you receive a call inviting you to input 2FA codes, you should hang up. Never send those codes to anyone. Instead, log into those services to monitor your activity. And call customer support. You might want to change the e-mail associated with that account to prevent these attacks from happening. Once hackers know what e-mail you use for PayPal or Bank of America, they might still target you with similarly sophisticated attacks.

There are other ways hackers might overcome 2FA protection. SMS intercepts are when hackers re-route text messaging to their own devices, so that your response to the 2FA request actually goes to the "bad guy" who then can access your account. A Supply Chain hack is when malware is inserted into software, like the SolarWinds hack earlier this year, that circumvents protection by removing the actual need for this authentication or again re-routing the request to a different party. Another ruse is called Workflow by-pass, which lets hackers modify passwords to lock out a user, then monitor the "reset" request and capture the credentials giving them access to the account. Pass-the-Cookie attacks use a ploy when users stored login credentials on browser cookies and the hacker would be able to "read" this information (which the industry has said has been corrected so this should no longer be a danger.) Finally, server-side forgeries was used for the Microsoft Exchange hack this year where malware over-wrote authentication completely so the "secure" log-in was moot.

MFA technology should be a part of corporate security's critical infrastructure. Recent attacks, as well as urging from experts across government and the private sector, should provide further impetus for intelligent implementations. However, these exploits show it is not 100% the answer for security. But, this does not mean you should not implement this security feature, as it will deter the "casual" hacker who does not have the advanced tech skills these other exploits require. Call SIM2K for information on using multi-factor authentication and ways to educate employees on potential dangers.

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