SIM2K
Adapting Technology to Your Business Needs

8•18
Information you can use

SIMformation

Is it Chrome or Nothing?

In the "browser wars" between Internet Explorer+Edge, Firefox and Chrome, Microsoft's and Mozilla's browsers fell to new lows in July as users continued to switch to Google's Chrome, which looks unstoppable.

According to analytics vendor Net Applications, Microsoft's Internet Explorer (IE) and Edge dropped to a combined user share of 15.4% last month, down a whopping 3.8 percentage points from June. Meanwhile, Mozilla's Firefox fell a much smaller two-tenths of a percentage point, recording a user share of 9.7%. Microsoft's July number was a record low in tracking of browser data dating back to 2005. Firefox's figure was its smallest user share since February 2006.

IE and Firefox usage problem is not new: Both companies have watched their once-substantial user share shrink over the last decade.

Microsoft's troubles appeared more dire, as its IE and Edge have shown few signs of stanching their continued losses. Of the past 24 months, IE and Edge lost share in 19. In the last year, the IE and Edge user share dropped by 6.8 percentage points, a 31% decline from the July 31, 2017 mark.

Firefox is struggling, too. July was the third consecutive month in which it posted a number under the 10% mark. In the past year, Firefox has lost 2.6 percentage points, or 21% of its July 31, 2017, user share.

Losses like Microsoft's and Mozilla's do not bode well for their future. If the trends of the last 12 months continue and IE and Edge lose another 31% in the next year, they will account for just 10.6% of the world's browser user share by this time in 2019. If Firefox again drops by 21%, it will fall to 7.6% in the same period.

Interestingly, Firefox may have the best shot at beating that prediction. That's because Firefox survived a "near-death" experience somewhat recently to bounce back to some degree. Two years ago this month, Net Applications reported that Firefox's user share had sunk to a record low of just 7.7%. But over the next year and two months, the browser clawed itself back to 13.1%. (Since October 2017, Firefox has lost share in all but one month.)

Microsoft's Internet Explorer (pre-Edge times) had a come-back, too: IE climbed from a December 2011 flirtation with 50% to grow to 59.1% three years later. But IE, and then IE + Edge, have lost ground, first slowly, then more rapidly, since December 2014. In other words, Microsoft's browser slide has been on-going for more than three and a half years, significantly longer than Firefox's nine-month decline.

The future of IE and Edge look nearly as ominous if the user share calculation considers their place within the Windows ecosystem, the only platform available to the browsers. According to Net Applications, IE and Edge accounted for 17.4% of the browsers that ran on Windows in July. (The 17.4% was larger than the 15.4% IE and Edge tallied overall because Windows does not power 100% of all PCs; in July, it ran 88.4% of the world's systems.) And trends are not in favor of IE, as it is already relegated to legacy status, and will increasingly be eliminated by commercial customers as they adopt Windows 10 and modernize the web apps and websites that now require them to support the old browser. That will leave Edge as the only competitive browser in Microsoft's arsenal.

And Edge remains a flop. In July, just 11.5% of all Windows 10 users relied on Edge, a record low for the browser. To get an idea of Edge's loose hold on Windows 10, consider that the browser was being used by almost twice the percentage of 10's owners, 20.4%, only 12 months ago.

In the browser battle, these losses became Google's gains: Chrome added nearly 4 percentage points to its user share in July, ending at 64.7%. The last time a browser owned that large a chunk of the world's browser market was in late 2009, when IE accounted for two-thirds of the total.

Calculations put Chrome on a faster track to that same two-thirds dominance. Using the average monthly change over the past 12 months, experts believe Chrome will reach 66.7% share or more in December and make it to 70% by August 2019. The 12-month average for IE+Edge and Firefox paint a different picture. IE and Edge will account for less than 12% of all user share by February 2019, then fall under 10% by May. Firefox will continue its decline as well, slipping below 9% in November and dipping under 8% in March 2019.

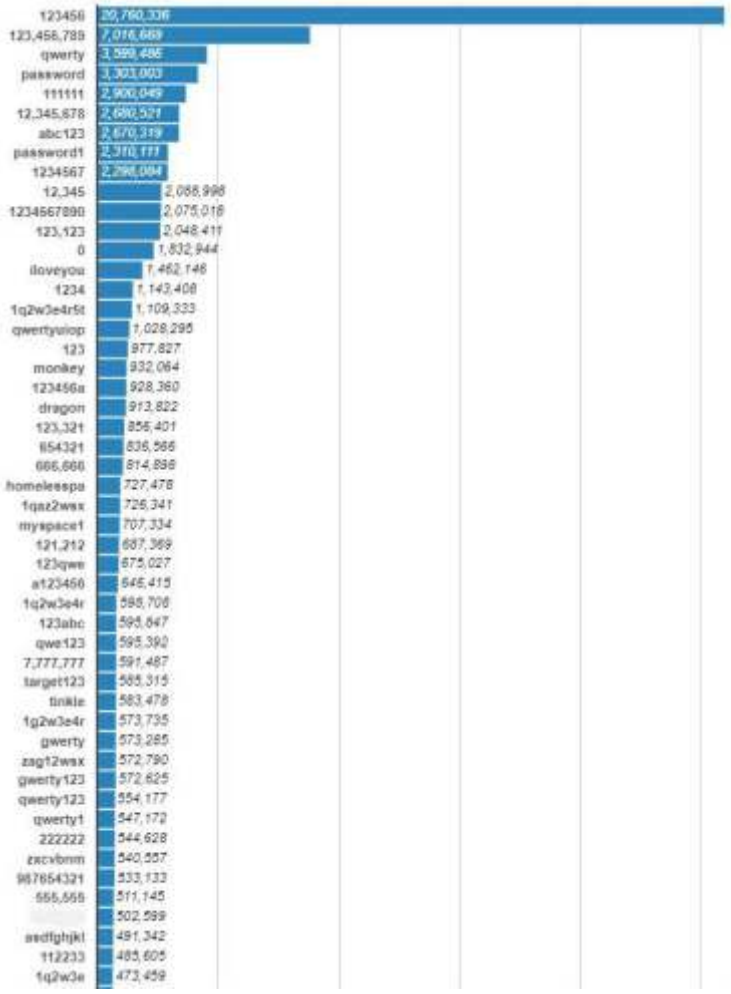
And not to be ignored, the numbers for Apple's Safari fell for the third straight month, ending at 3.5%, its lowest since April 2017. Safari's share of all macOS-powered systems also dropped to 38.3% in July, indicating that being an operating system's default browser no longer guarantees success.

People are making independent choices on what Internet browser they wish to use, and overwhelmingly the choice today is Google's Chrome. While we will not comment on whether this is a good choice, there are many IT people out there that believe that Google is building a massive database of user experience and browsing history and using Chrome just plays into that data trove. So who still has their old Netscape installation diskettes?

50 Most Exposed Passwords

Coming up with the "perfect password" is often hard, as it must be something you will remember, but it also has to be complex to help fend off hackers trying to guess your credentials. The site Have I Been Pwned keeps track of data breaches and stolen credentials. It recently published a list of the most vulnerable passwords found in breaches, which is shown below. (One password is blurred as it uses the F-bomb and we are a family publication...!)

Password management and safety mean you should have a unique password using a mix of upper- and lower-case letters, number and characters. A common substitution has been to use the character @ in lieu of an "a" in a string, so this tactic is becoming too well known to continue to recommend doing. Also, while it may lead to a confusing mishmash of passwords, you should have separate passwords for different sites, especially a unique password for any on-line banking or other financial websites you access. Don't use your Facebook or Yahoo login for your banking, to try to minimize the possibility of a data breach exposing your personal information. Call SIM2K for help in establishing a secure password scheme and for information on two-factor authentication tools for added security for your accounts.



Security Keys an Option

No Google employee has fallen prey to phishing attacks since early 2017, which is when the company started requiring all its workers to use physical security keys. Physical security keys, which are sold for as low as $20, are inexpensive USB-based devices that may be used to shore up user security. In the case of Google, it appears that investing in these devices is paying off.

Google says that none of the company's 85,000+ employees have fallen victim to a phishing attack on their work accounts since the company began requiring them to use physical security keys in place of traditional passwords and one-time codes. "We have had no reported or confirmed account takeovers since implementing security keys at Google," said a Google spokesperson.

Security keys are inexpensive devices that provide an alternative to two-factor authentication, a security technique requiring users to provide the password and then sends another code to their smartphone that must be entered to unlock the account.

Phishing attacks come in various forms, but their end goal is to trick users into giving up sensitive information such as log-in details. Two-factor authentication seeks to prevent this, because even if hackers acquire an account's password, they will also need to acquire the second code.

The physical security key makes it harder for hackers to acquire that second factor. It authenticates log-ins by being inserted into the computer's USB port, with the user then pressing a button on it. This means that hackers will need to have the security key in their actual possession.

There are various ways to protect against phishing, including the simple way of not responding to suspicious e-mails. However, introducing two-factor authentication and adding a physical security key offer greater protection. SIM2K offers our Duo two-factor authentication service, and can source physical security keys if you want to add this protection, as well. Typically, a security key runs about $20 each, so if you have a large staff it might be a cost matter to do this, but that is still "small change" vs. a hacker obtaining your banking information from an unsuspecting employee and draining your account. SIM2K also offers security testing wherein we can stage a mock attack on your employees to see if any do respond, and thus need additional counseling on cybersecurity methods, as well as other security options depending on your needs. Remember, there is no price for an impenetrable wall of cybersecurity this day and age.

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 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Cloud Security

The march toward the cloud for data and services has many companies rethinking their approach to cyber security. Do they need a cloud security strategy? What is different about a cloud security strategy? Recent surveys have shed light on how security strategies are changing, and more important, how they should change.

Some people feel that moving to the Cloud can be more secure than in house. For instance, Cloud providers are probably running the latest software version with the proper patches in place. Cloud service providers are also building in new capabilities such as using machine language for anomaly detection. Not all businesses are as diligent on their updates and patches. However, it also presents new risks, some of which is the result of misunderstanding how to manage cloud security.

Data from cloud security provider Alert Logic shows the nature and volume of risk for each form of cloud environment as compared to an on-premises data center. For 18 months, the company analyzed data from more than 3,800 customers to quantify and categorize security incidents. During that time, it identified more than 2.2 million true positive security incidents. Key findings include:

- Hybrid cloud environments experienced the highest average number of incidents per customer at 977, followed by hosted private cloud (684), on-premises data center (612), and public cloud (405).
- By far, the most common type of incident was a web application attack (75%), followed by brute force attack (16%), recon (5%), and server-side ransomware (2%).
- The most common vectors for web application attacks were SQL (47.74%), Joomla (26.11%), Apache Struts (10.11%), and Magento (6.98 %).
- Wordpress was the most common brute force target at 41%, followed by MS SQL at 19%.

To minimize the impact from cloud threats, here are some recommendations:

- Rely on application whitelisting and block access to unknown programs. This includes doing risk vs. value assessments for each app used in the organization.
- Understand your own patching process and prioritize deployment of patches.
- Restrict administrative and access privileges based on current user duties. This will require keeping privileges for both applications and operating systems up to date.

Not every company is migrating sensitive or critical data to the cloud, so for them there is less reason to change strategy. However, most companies are migrating critical and proprietary company information (56%) or marketing assets (53%). 47% expect to have personally identifiable information in the cloud, which has implications due to new privacy regulations such as the EU's GDPR. So if you are moving data to the Cloud, in any configuration of public, private or hybrid, consider your security posture independent of your in-house network policies.

"Random Tid-Bytes"

Zultys for iPhones

Zultys has announced that the new version of the Zultys Mobile application for iPhone is available to download from iTunes App Store. This release adds the ability for members of a Group Chat to initiate a conference call with all their fellow team members with a single button. This feature allows team members to collaborative more effectively regardless of whether they are using ZAC application on their computer or are connecting via an iOS device. Another new feature is the addition of On-Demand Call Recording to the mobile application. Recordings can be initiated from the application's answer screen with a tap of a button. The recording will capture the conversation from the beginning regardless of when the user presses the button. After the call is completed, the recording can be accessed right away from both Zultys Mobile and the user's ZAC application on their computer. The new Zultys Mobile app for iPhones can be downloaded from the iTunes store. As an authorized Zultys partner, SIM2K can help you with integrating your mobile phones into your Zultys system, so call us for information.

PC Sales Show Uptick

Despite some views that tablets and smartphones would replace PCs as the "go too" tech tool, IDC reports that PC sales showed an uptick in sales for Q2 of this year. Shipments of new PCs rose 2.7% over Q2 of 2017, the strongest quarterly growth since Q1 2012. Sales were up last quarter for all five of the major manufacturers – HP, Lenovo, Dell, Apple and Acer. HP leads the market with a 23.9% share, followed by Lenovo with 22.1%. Lenovo's growth was sparked in part by taking over the PC business from Fujitsu. Dell saw 18.1% share, and Apple at 6.9%. Insiders believe Apple sales will stagnate now until the update for the MacBook line is released later this year. Gartner, though, was more pessimistic. "PC shipment growth in the second quarter of 2018 was driven by demand in the business market, which was offset by declining shipments in the consumer segment," said an analyst at Gartner. "In the consumer space, ... (they) are using their smartphones for even more daily tasks, such as checking social media, calendaring, banking and shopping, which is reducing the need for a consumer PC." In the U.S., Gartner said PC sales increased 1.7% to 14.510 million units. HP, Dell, Lenovo, Apple, and Acer maintained their positions. Gartner does not count Chromebooks as PCs, whereas IDC does.

SIM2K and Epson Brighter Futures

SIM2K is now able to offer educational solutions for classroom projectors such as the Brightlink Interactive Projector shown here. With our partnership with Epson and their Brighter Futures program, we are able to offer special pricing for schools, school districts or other related agencies. Enhance every student's learning experience with dynamic, user-friendly imaging technology that invites participation and engages viewers in any environment, whether it's a classroom, lab or gymnasium. From advanced displays, projectors, printers and scanners, Epson and SIM2K can provide you with a comprehensive suite of education solutions to meet any need. Call us for more information.

Cybersecurity Still Critical

The cyberattack on the Equifax credit reporting agency in 2017, which led to the theft of Social Security numbers, birth dates, and other data on almost half the U.S. population, was a stark reminder that hackers are thinking big when it comes to targets. Other companies that hold lots of sensitive information continue to be targeted as the hackers continue to look for ways to access your information. Security experts believe that data brokers who hold information about things such as people's personal Web browsing habits will be especially popular targets in addition to social media sites with lots of people using weak passwords. Here are some of the areas experts believe are current targets for the "bad guys."

Ransomware in the cloud

The past 12 months have seen a plague of ransomware attacks, with targets including Britain's National Health Service, San Francisco's light-rail network, and big companies such as FedEx. Ransomware is a relatively simple form of malware that breaches defenses and locks down computer files using strong encryption. Hackers then demand money in exchange for digital keys to unlock the data. Victims will often pay, especially if the material encrypted hasn't been backed up.

That's made ransomware popular with criminal hackers, who often demand payment in hard-to-trace cryptocurrencies. Some particularly vicious strains, such as WannaCry, have compromised hundreds of thousands of computers. One big target is cloud computing businesses, which house mountains of data for companies. Some also run consumer services such as e-mail and photo libraries. The biggest cloud operators, like Google, Amazon, and IBM, have hired legions of digital security experts, so they won't be easy to crack. But smaller companies are likely to be more vulnerable, and even a modest breach could lead to a big payday for the hackers involved.

The weaponization of Artificial Intelligence

This year has seen the emergence of an AI-driven arms race. Security firms and researchers have been using machine-learning models, neural networks, and other AI technologies for a while to better anticipate attacks, and to spot ones already under way. It's highly likely that hackers are adopting the same technology to strike back. "AI unfortunately gives attackers the tools to get a much greater return on their investment," says anti-virus company McAfee.

An example is spear phishing, which uses carefully targeted digital messages to trick people into installing malware or sharing sensitive data. Machine-learning models can now match humans at the art of crafting convincing fake messages, and they can churn out far more of them without tiring. Hackers will take advantage of this to drive more phishing attacks. They're also likely to use AI to help design malware that's even better at fooling "sandboxes," or security programs that try to spot rogue code before it is deployed in companies' systems.

Cyber-physical attacks

More hacks targeting electrical grids, transportation systems, and other parts of countries' critical infrastructure are taking place in 2018. Some are designed to cause immediate disruption, while others will involve ransomware that hijacks vital systems and threatens to wreak havoc unless owners pay swiftly to regain control of them. During the year, researchers – and hackers – are likely to uncover more chinks in the defenses of older planes, trains, ships, and other modes of transport that could leave them vulnerable.

Mining cryptocurrencies

Hackers, including some allegedly from North Korea, have been targeting holders of Bitcoin and other digital currencies. But the theft of cryptocurrency isn't the biggest threat to worry about in 2018; instead, it's the theft of computer processing power.

Mining cryptocurrencies requires vast amounts of computing capacity to solve complex mathematical problems. That is encouraging hackers to compromise millions of computers in order to use them for such work. Recent cases have ranged from the hacking of public Wi-Fi in a Starbucks in Argentina to a significant attack on computers at a Russian oil pipeline company. As currency mining grows, so will hackers' temptation to breach many more computer networks. If they target hospital chains, airports, and other sensitive locations, the potential for collateral damage is deeply worrying.

Hacking elections (again!)

Fake news isn't the only threat facing any country running an election. There's also the risk of cyberattacks on the voting process itself. It's now clear that Russian hackers targeted voter registration databases in numerous American states ahead of the 2016 presidential election. With midterm elections looming in the U.S. in November, officials have been working hard to plug vulnerabilities. But determined attackers still have plenty of potential targets, from electronic voter rolls to voting machines and the software that's used to collate and audit results.

As these and other risks grow in 2018, so will the penalties for companies that fail to address them effectively. On May 25, the General Data Protection Regulation came into effect in Europe. The first big overhaul of the region's data protection rules in more than two decades, the GDPR requires companies to report data breaches to regulators – and inform customers their data has been stolen – within 72 hours of discovering a breach. Failure to comply could lead to fines of up to 20 million euros or 4% of a company's global revenues, whichever is greater.

The recent revelation that Uber covered up a big cyberattack last year has sparked calls for breach disclosure rules to be toughened in America too. All this means that cybersecurity will continue to be of utmost importance as there is no sign that the hackers and malware attacks will be brought under control at any time soon. Call SIM2K for help in conducting vulnerability assessments and hardening your network security before you are attacked.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com