

DIGITAL SHADOWS ANNOUNCES ALEX SETON AS VP BUSINESS AND CORPORATE DEVELOPMENT

DUBAI: Digital Shadows, the industry leader in external digital risk management, announced the appointment of Alex Seton as Vice President of Business and Corporate Development to further accelerate industry adoption of Digital Shadows solutions through an innovative partner eco-system, investment and go-to-market approach.

With over 24 years of experience, Alex is well known in the cyber security industry for identifying and delivering compelling product solutions and strategic partnerships resulting in increased customer value and company acceleration. As founding VP of Business Development, Channels, and Strategic

Alliances at network security analytics pioneer Solera Networks, Alex developed the industry's first Advanced Threat Protection eco-system with a highly successful partnering approach evidenced by success for customers, strategic partners and investors alike.

Alex also served as VP Corporate Development at Blue Coat Systems and held executive roles Cisco LANDesk, and Novell. "We are delighted to welcome Alex to join the Digital Shadows family and help us build a world-class global business development strategy to further protect customers around the globe with our unique offering and further accelerate our market penetration," said

Alastair Paterson, CEO and Co-Founder of Digital Shadows. "I am confident he will help us to drive the build out of a robust global partner eco-system by developing industry differentiating technology partnerships and global strategic commercial partnerships.

"Today's digital economy indexed on the use of digital technologies requires that organizations gain situational awareness into their digital footprint to understand their external risk exposure and enable threat mitigation actions. Such a holistic approach requires collaboration and integrations. Through Alex's industry knowledge, experience and past success in developing strategic

partner eco-systems, we expect Digital Shadows customers to benefit in even greater terms through streamlined workflows and increased product availability," said Doug Cahill, Senior Analyst, Enterprise Strategy Group.

Digital Shadows finished 2016 with its third consecutive year of triple-digit revenue growth, and experienced significant customer expansion in both the United States and Europe, across verticals such as financial services, pharmaceuticals, retail, and technology. The company expanded rapidly, reaching 100 employees in the second half of 2016 and opening a new office in Dallas to add to the sites in San Francisco and London.



Alex Seton, VP Business and Corporate Development, Digital Shadows



SINGAPORE: This photograph shows workers under the care of the Transient Workers Count Too welfare group show off their new 3G phones and the 2G phones they swapped them for, at a restaurant in Singapore. — AFP

NEEDY EXPAT WORKERS GET PHONES AS SINGAPORE MOVES TO SCRAP 2G

NEW PHONES HELP EXPATS REACH THEIR FAMILIES

SINGAPORE: A Singapore migrant welfare group has started distributing 3G-enabled mobile phones to cash-strapped foreign workers days before the city-state shuts down its 2G network. Telecom operators in the highly wired island will end second-generation services on April 1, forcing thousands still relying it to upgrade their handsets or become a casualty of technology's relentless advance. Migrants group Transient Workers Count Too (TWC2) said the first batch of handsets was given to 50 jobless foreign workers late Tuesday.

The laborers are out of work due to wage disputes or workplace injury. Many rely on cheap 2G handsets to keep in touch with loved ones back home while awaiting a resolution to their problems. TWC2 said it would hand out 120 more handsets next week, while some of the remaining 80 phones

which have been collected would be given to other migrant welfare groups for distribution. The group had urged the public to donate used 3G handsets or money to buy phones for the workers.

Singapore, with one of the world's highest mobile penetration rates, is re-allocating scarce radio frequency spectrum to meet surging consumer demand for high-speed data. But some 132,300 people in the city-state were still using 2G phones as of December, official data showed. "Phones are a lot more important to these workers than to all of us who have access to computers. It's their only link to their family... a very important social lifeline for them," TWC2 treasurer Alex Au said.

There are almost 1.4 million foreign workers in labor-scarce Singapore, many in the construction and marine industries. Bangladeshi

Ahamed Mohammad Faruk, 30, who has been jobless for eight months after his employer withheld his salary, was among those who got a phone. He had been wondering how his three-year-old daughter has grown since he left for Singapore two years ago with just a few pictures of her. His old 2G phone could only be used for calls and texting.

"I am excited to see her (recent) pictures," a smiling Ahamed said after getting a touchscreen phone that can send and receive multimedia and browse the internet. Japan, South Korea and US telecom giant AT&T have already shut down their 2G networks and Australia is set to stop the service in September. But globally, 2G is not set to vanish, even as the number of smartphones is projected to soar from four billion last year to some six billion by 2020, according to IHS Markit data. — AFP

MANAGEENGINE TO ADVANCE BUSINESS IT ALIGNMENT WITH HELP FROM ZOHU

DUBAI: ManageEngine, the real-time IT management company, yesterday announced its strategy for advancing the state of IT management and aligning IT with business objectives. Parent company Zoho Corporation plays a key role in the plans as ManageEngine will integrate Zoho's cloud-based business apps with the industry's broadest suite of IT management software. ManageEngine will continue to evolve its applications based on lessons gained from managing the Zoho Cloud, one of the largest public clouds in the world, and will continue to work on the contextual integration of the ManageEngine suite.

Relentless advances in cloud computing, mobility and other technologies are creating new opportunities and challenges for end-user organizations. However, IT teams are often hamstrung by multi-vendor IT management solutions that are functionally disconnected from each other and isolated from the rest of the organization. In turn, IT teams and business units grow further out of sync as IT teams take longer to act on new opportunities while business productivity and continuity suffer, leaving business units to watch opportunities slip away.

"The future of IT is the intersection of technology and business," said Raj Sabhlok, president of ManageEngine. "Most IT decisions are being made at the line of business or are being influenced at the line of business. IT teams need a suite of integrated tools that can help them work at that level, and we are uniquely qualified to deliver that suite. Zoho is the operating system for business and lives at the line of business. Working even more closely with Zoho puts ManageEngine where we need to be - helping to develop, deploy, manage and secure these critical business applications."

Bringing IT Together

ManageEngine has built more than 90 IT management applications and free tools.

Taken together, the suite provides everything an IT department needs to affordably manage all of its IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

In its efforts to improve IT manageability, ManageEngine has already begun contextually integrating many of its applications, sharing data across applications and enabling IT pros to perform relevant functions of one application from the UI of another. To date, such contextual integrations have been created for its desk, desktop, mobile device, and operations management solutions. The expanded ManageEngine-Zoho relationship promises to push IT-business alignment to new levels.

The IT community has already caught a glimpse of this alignment in the form of Analytics Plus, ManageEngine's self-service IT analytics platform that is powered by Zoho's business technology. Later this month, the company will roll out a solution that unites one of its IT management applications with customer account management and billing apps from Zoho. Going forward, the two companies will deliver other integrations to help organizations tightly align their IT operations and business strategies. Meanwhile, IT teams can leverage Zoho Creator, the low-code app development platform, to rapidly build and launch custom, mobile-ready apps.

To signal closer affinity with Zoho, ManageEngine has refreshed its website and logo. The new website touts the company's work in "Bringing IT together," emphasizing its ability to manage any company's entire IT environment and, going forward, align their IT and business. The website has also been updated and streamlined to improve usability. In addition, the ManageEngine logo has been updated with a new crest that includes the red, green, blue and yellow colors of Zoho.



Raj Sabhlok, President ManageEngine, left, and Nirmal Manoharan, Regional Director of sales ManageEngine.

ONE IN FOUR WI-FI HOTSPOTS JUST WAITING TO BE HACKED

DUBAI: After analyzing information on more than 31 million Wi-Fi hotspots around the world, Kaspersky Lab has found that every fourth (28 percent) is unsecured and poses a risk to users' personal data. That means all the traffic transmitted over those networks, including personal messages, passwords, documents and much more, can be easily intercepted and used by attackers.

According to Kaspersky Security Network, 25 percent of the world's Wi-Fi networks have no encryption or password protection of any kind. In other words, the information they transmit is completely open and can be read by third parties. Another 3 percent of hotspots use WEP (Wired Equivalent Privacy) to encrypt data. This unreliable protocol can be "cracked" within minutes using tools that are freely available on the Internet.

The rest of the nearly three-quarters of Wi-Fi hotspots use a more reliable form of encryption based on the family of Wi-Fi Protected Access (WPA) protocols. The effort required to hack these networks depends on the settings, including the strength of the password. For instance, if it's a weak or publicly accessible password (e.g., on display in a cafe), a criminal will also be able to decrypt any transmitted traffic.

It's worth noting that the top 20 countries with the highest percentage of non-encrypted Wi-Fi hotspots includes many popular tourist destinations - Thailand, France, Israel, the US and so on. Travelers are among the most vulnerable because the nearest available Wi-Fi hotspot is often the only way for them to stay connected. At the same time, another study suggests only 52 percent of Internet users in the UAE are concerned about their data being intercepted during a Wi-Fi session.

"We advise all users to remain vigilant when connecting to Wi-Fi. Don't use hotspots without passwords and don't use public hotspots to perform high-risk activities such as online banking or shopping, logging on to sites or for transferring confidential information. If that sort of traffic is intercepted by a third party, it could result in serious losses, including financial losses. And of course, we strongly recommend using additional measures to protect traffic, such as VPN (Virtual Private Network) technology," explains Denis Legezo, Antivirus Expert at Kaspersky Lab.

The flagship solutions Kaspersky Internet Security and Kaspersky Total Security now integrate the new Secure Connection feature that encrypts all data sent and received over a communication channel. Depending on the user settings, Secure Connection can be run automatically when attempting to connect to an unsecured network, or when performing potentially vulnerable operations online.

AIRLINE PASSENGERS HIT THE DEVICE DOLDRUMS

NEW YORK: As the indignities of modern air travel go, the latest ban on laptops and tablets on some international flights falls somewhere between having to take off your ratty shoes at the security checkpoint and having your baby food and milk tested for bomb residue. It's yet another inconvenience in the name of security for weary travelers, especially those from or passing through the 10 mostly Middle Eastern and North African countries covered by new US and British policies.

While it's not quite as disruptive as an outright ban on smartphones - much less a travel ban based on nationality - the laptop limitation loomed large for some people as they prepared to travel. "Why are only Middle Eastern airlines subject to this ban?" asked Kelsey Norman, a doctoral student who plans to fly home Friday to Los Angeles from Beirut - and expects to have to check her laptop, a Kindle tablet and her DSLR camera. "Overall this policy is inconvenient, discriminatory, and continues to hurt America's rapidly deteriorating reputation globally."

Ban logic
The US Department of Homeland Security rules for-



FRANKFURT: In this file photo, a new Qatar Airways Airbus A350 approaches the gate at the airport in Frankfurt, Germany. — AP

bid laptop computers, tablets, Kindles, some gaming devices, cameras and other electronics larger than a smartphone in carry-on baggage. The US government cited unspecified threats as the reason for the ban. The UK government instituted a similar ban; neither government's restrictions affect US-based airlines.

On the positive side, items people can still carry into the airline cabin include smartphones, overstuffed duffel bags, winter coats, tiny bottles of hand lotion, Tupperware containers full of tuna salad, earplugs, nose hair trimmers, and babies. For now, at least - tomorrow could bring a new unspecified threat and with it a new ban.

Lost productivity

Other travelers, especially of the dutiful business variety, worried that laptops in checked bags could be stolen, damaged or compromised - and that in the meantime, they wouldn't be able to get any work done. Some tried rerouting flights to avoid the affected airports, but this is not easy. Banu Akdenizli, a native of Turkey, said having to fly 17 hours without her laptop will cost her precious time to work and prepare for a conference.

Awkward workarounds

If you're someone who insists on working, it's possible to take import documents into Google Docs and thumb away on your smartphone's keyboard, at least so long as you remember to save them to your phone before you take off. But features can be limited with some apps; Microsoft's Office app, for instance, only lets you open one document at a time. Such apps are OK for simple proofreading and minor editing, but probably won't do if you're working on your novel.

Among other things, the text is tiny when fitting a full page on a phone's screen, though there's a button to temporarily reformat text for the smaller display. Catching up on email or cleaning out your inbox could be another way to pass time without your laptop, especially if you shell out for in-flight Wi-Fi. If you can resist the urge to work, you can download shows from Netflix or Amazon onto your phone for offline viewing - though again, you have to remember to do this before your flight. And you might want to stick with comedies or TV shows rather than epics designed for big screens.

At least it's not phones

For most of us, laptops and other gadgets play mere supporting roles compared to our extra limb, our one and only - the smartphone. We go to sleep with it and look at it the first thing in the morning. Had the ban included smartphones, passengers might now be agitating for the return of zeppelin travel. Last fall, Samsung asked users of its fire-prone Galaxy Note 7 to "power down and stop using the device" when getting on a plane. (The phone was later banned, and then recalled.) People followed the directions but found clever workarounds, such as borrowing non-Note 7 phones from friends. — AP